IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

FINJAN SOFTWARE, LTD., an Israel corporation, Plaintiff, v. SECURE COMPUTING CORPORATION, a Delaware corporation, CYBERGUARD, CORPORATION, a Delaware corporation, WEBWASHER AG, a German corporation and DOES 1 THROUGH 100, Defendants.	)	C. A. No. 06-369-GMS **PUBLIC VERSION**

DECLARATION OF LISA KOBIALKA IN SUPPORT OF PLAINTIFF FINJAN SOFTWARE, LTD.'S POST-TRIAL MOTION FOR ENTRY OF PERMANENT INJUNCTION PURSUANT TO 35 U.S.C. § 283

VOLUME 2 – EXHIBITS 22-32

OF COUNSEL:

Paul J. Andre
Lisa Kobialka
King & Spalding LLP
1000 Bridge Parkway
Redwood City, CA 94065
(650) 590-0700

Dated: April 25, 2008
Public Version: May 2, 2008

Philip A. Rovner (#3215)
POTTER ANDERSON & CORROON LLP
Hercules Plaza
P. O. Box 951
Wilmington, DE 19899
(302) 984-6000
provner@potteranderson.com

Attorneys for Plaintiff
Finjan Software, Ltd.

I, LISA KOBIALKA, declare:

1. I am an Partner with the law firm of King & Spalding LLP, counsel of record for Finjan Software, Ltd ("Finjan"). I have personal knowledge of the facts set forth in this declaration and can testify competently to those facts.

2. Attached hereto as Exhibit 1 is a true and correct copy of trial exhibit JTX-1, U.S. Patent No. 6,092,194.

3. Attached hereto as Exhibit 2 is a true and correct copy of trial exhibit JTX-2, U.S. Patent No. 6,804,780.

4. Attached hereto as Exhibit 3 is a true and correct copy of trial exhibit JTX-3, U.S. Patent No. 7,058,822.

5. Attached hereto as Exhibit 4 is a true and correct copy of pages 183-184, 186-187, 207, 214-222, 286-290 306, 313-314, 318-319, 329-333, 415-417, 436-437, 456-458, 597-609, 671-672, 674-679, 692-701, 712, 736-738, 1207, 1209-1210, and 1232 from the trial transcript in the present case, Finjan Software Ltd. v. Secure Computing Corp., Civil Action No. 06-369 GMS.

6. Attached hereto as Exhibit 5 is a true and correct copy of pages 66-67 from the deposition transcript of Shlomo Touboul, dated October 23, 2007.

7. Attached hereto as Exhibit 6 is a true and correct copy of trial exhibit PTX-23, a document entitled "IDC Market Analysis: Worldwide Antivirus Software Forecast and Analysis, 2003-2007: Return of the Consumer" bearing bates numbers SC072833-68.

8. Attached hereto as Exhibit 7 is a true and correct copy of trial exhibit PTX-21, a PowerPoint Presentation entitled "Webwasher SCM 6.0-Anti-Malware: New Features as of Release 6.0" bearing bates numbers SC066200-21.

9. Attached hereto as Exhibit 8 is a true and correct copy of trial exhibit PTX-31, an email from Martin Stecher dated September 16, 2002, bearing bates numbers SC077630-31.

10. Attached hereto as Exhibit 9 is a true and correct copy of trial exhibit PTX-16, an email from Christoph Alme to Martin Stecher dated May 28, 2004, bearing bates numbers SC166301-02.

11. Attached hereto as Exhibit 10 is a true and correct copy of trial exhibit DTX-1056, an document entitled "Product Meeting Minutes," bearing bates numbers SC075246-48.

12. Attached hereto as Exhibit 11 is a true and correct copy of a press release entitled "Secure Computing Responds to Finjan Patent Infringement Lawsuit Verdict," dated March 13, 2008, *available at* http://www.tradingmarkets.com/.site/news/Stock%20News/1199018.

13. Attached hereto as Exhibit 12 is a true and correct copy of a webpage from the Secure Computing website entitled "Secure Web," available at http://www.securecomputing.com/index.cfm?skey=22&land=en, last viewed on April 25, 2008.

14. Attached hereto as Exhibit 13 is a true and correct copy of trial exhibit PTX-34, an email from Peter Borgolte regarding Product Meeting Minutes dated September 16, 2003, bearing bates numbers SC077703-05.

15. Attached hereto as Exhibit 14 is a true and correct copy of pages 25-26 and 41-42 from the deposition transcript of Jill Putnam dated September 11, 2007.

16. Attached hereto as Exhibit 15 is a true and correct copy of trial exhibit DTX-1071, a document entitled "Finjan/Webwasher Competitive Analysis" dated April 2006, bearing bates numbers FIN014950-87.

17. Attached hereto as Exhibit 16 is a true and correct copy of trial exhibit PTX-33, a Webwasher AG paper entitled "Finjan SurfinGate Web 7.0 Competitive Analyses," dated May 20, 2003, bearing bates numbers SC153656-63.

18. Attached hereto as Exhibit 17 is a true and correct copy of trial exhibit PTX-36, an email from Horst Joepen dated June 18, 2004, bearing bates numbers SC166304-18.

19. Attached hereto as Exhibit 18 is a true and correct copy of trial exhibit PTX-35, an email from Ronald Cuny dated April 19, 2004, bearing bates numbers SC030765-66.

20. Attached hereto as Exhibit 19 is a true and correct copy of trial exhibit PTX-120, a document entitled "Why Companies Choose WebWasher EE Over Finjan," dated November 24, 2003, bearing bates numbers SC05090-96.

21. Attached hereto as Exhibit 20 is a true and correct copy of trial exhibit PTX-48, an email dated October 4, 2004, bearing bates numbers SC028994-96.

22. Attached hereto as Exhibit 21 is a true and correct copy of trial exhibit PTX-118, a document entitled "Webwasher Sales Manual" dated December 6, 2006, bearing bates numbers SC02676-770.

23. Attached hereto as Exhibit 22 is a true and correct copy of trial exhibit PTX-43, a document entitled "UBS Group Anti Virus Gateway Project" dated April 14, 2005, bearing bates numbers SC148034-62.

24. Attached hereto as Exhibit 23 is a true and correct copy of trial exhibit JTX-45, a document entitled "Secure Computing Annual Report 2006."

25. Attached hereto as Exhibit 24 is a true and correct copy of trial exhibit PTX-25, a document entitled "IDC Market Analysis: Worldwide Secure Content Management 2005-2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam and Malicious Code Continue to Wreak Havoc," dated September 2005, bearing bates numbers SC076359-440.

26. Attached hereto as Exhibit 25 is a true and correct copy of trial exhibit PTX-116, a document entitled "Webwasher Hot Sheet," bearing bates numbers SC 02370-71.

27. Attached hereto as Exhibit 26 is a true and correct copy of trial exhibit JTX-11, a document entitled Secure Computing Corporation Form 10-K for the Fiscal Year Ended December 31, 2006.

28. Attached hereto as Exhibit 27 is a true and correct copy of an IDC Market Analysis-Worldwide Secure Content and Threat Management 2007-2011 Forecast and 2006 Vendor Shares: 1+1=4 dated June 2007.

29. Attached hereto as Exhibit 28 is a true and correct copy of Secure Computing press release entitled "Secure Computing Files Motion to Set Aside Previous Infringement Verdict" dated March 28, 2008.

30. Attached hereto as Exhibit 29 is a true and correct copy of a webpage from the Secure Computing website titled "Technical Support," *available at* http://www.securecomputing.com/index.cfm?sKey=1312, last visited on April 25, 2008.

31. Attached hereto as Exhibit 30 is a true and correct copy of a press release entitled "Secure Computing Intros New WebWasher" dated September 24, 2007.

32. Attached hereto as Exhibit 31 is a true and correct copy of trial exhibit PTX-38, a document entitled "Proactive Security," bearing bates numbers SC155173-81.

34. Attached hereto as Exhibit 32 is a true and correct copy of an article entitled "Secure Computing Webwasher 6.0" dated February 1, 2007, *available at* http://www.scmagazineus.com/Secure-computing-Webwasher-60/printreview/612/, last visited on April 25, 2008.

I declare under penalty of perjury under the laws of the State of California and the United States that the foregoing is true and correct. Executed this 25th day of April 2008, at Redwood Shores, California.

Lisa Kobialka

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

CERTIFICATE OF SERVICE

I, Philip A. Rovner, hereby certify that on May 2, 2008, the within document was filed with the Clerk of the Court using CM/ECF which will send notification of such filing(s) to the following; that the document was served on the following counsel as indicated; and that the document is available for viewing and downloading from CM/ECF.

BY HAND DELIVERY AND E-MAIL

Frederick L. Cottrell, III, Esq.
Kelly E. Farnan, Esq.
Richards, Layton & Finger, P.A.
One Rodney Square
920 N. King Street
Wilmington, DE 19801
cottrell@rlf.com; farnan@rlf.com

I hereby certify that on May 2, 2008 I have sent by E-mail the foregoing document to the following non-registered participants:

Jake M. Holdreith, Esq.
Christopher A. Seidl, Esq.
Robins, Kaplan, Miller & Ciresi L.L.P.
2800 LaSalle Plaza
800 LaSalle Avenue
Minneapolis, MN 55402
jmholdreith@rkmc.com ; caseidl@rkmc.com

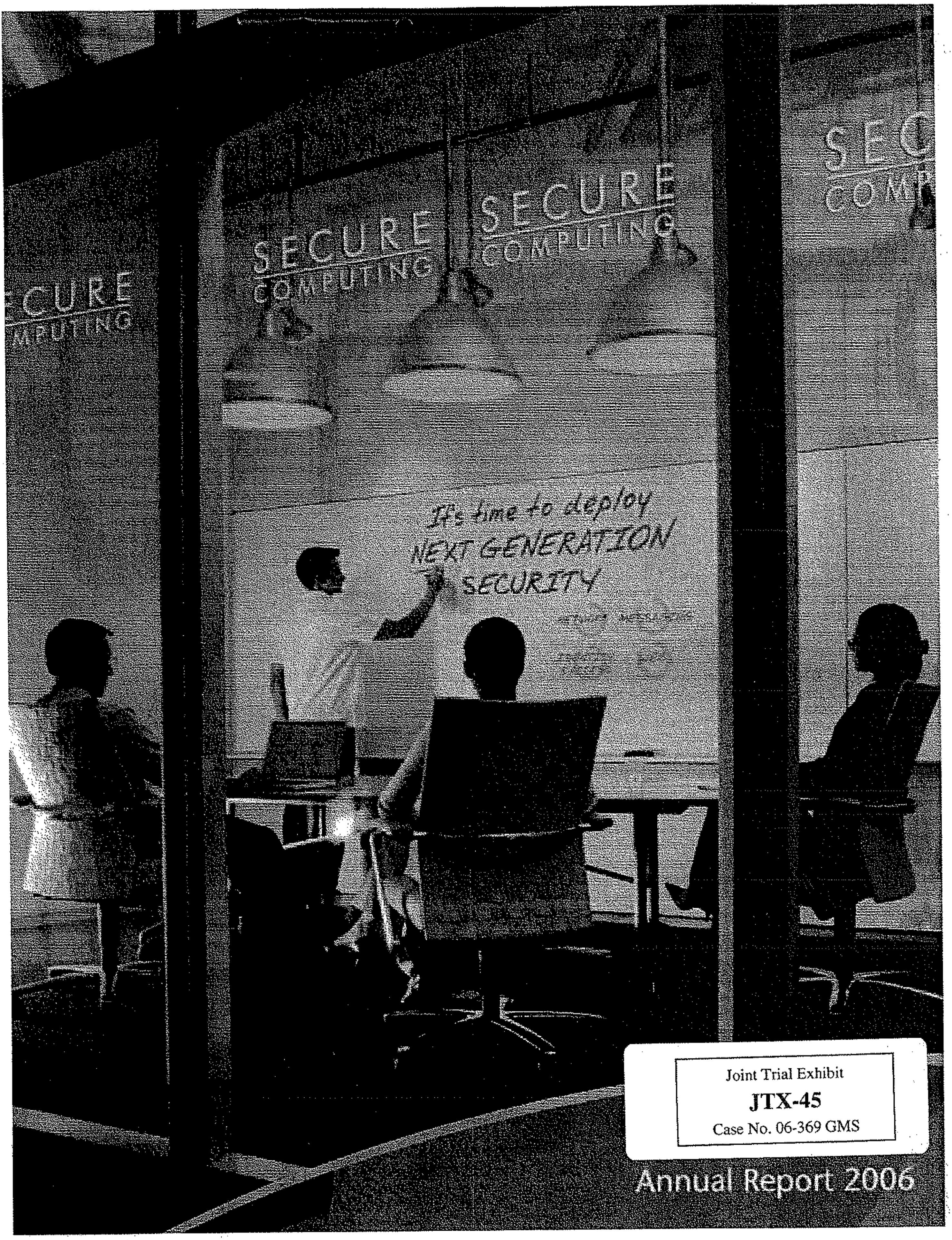
/s/ Philip A. Rovner
Philip A. Rovner (#3215)
Potter Anderson & Corroon LLP
Hercules Plaza
P.O. Box 951
Wilmington, Delaware 19899
(302) 984-6000
E-mail: provner@potteranderson.com

EXHIBIT 22

THIS EXHIBIT HAS BEEN
REDACTED IN ITS ENTIRETY

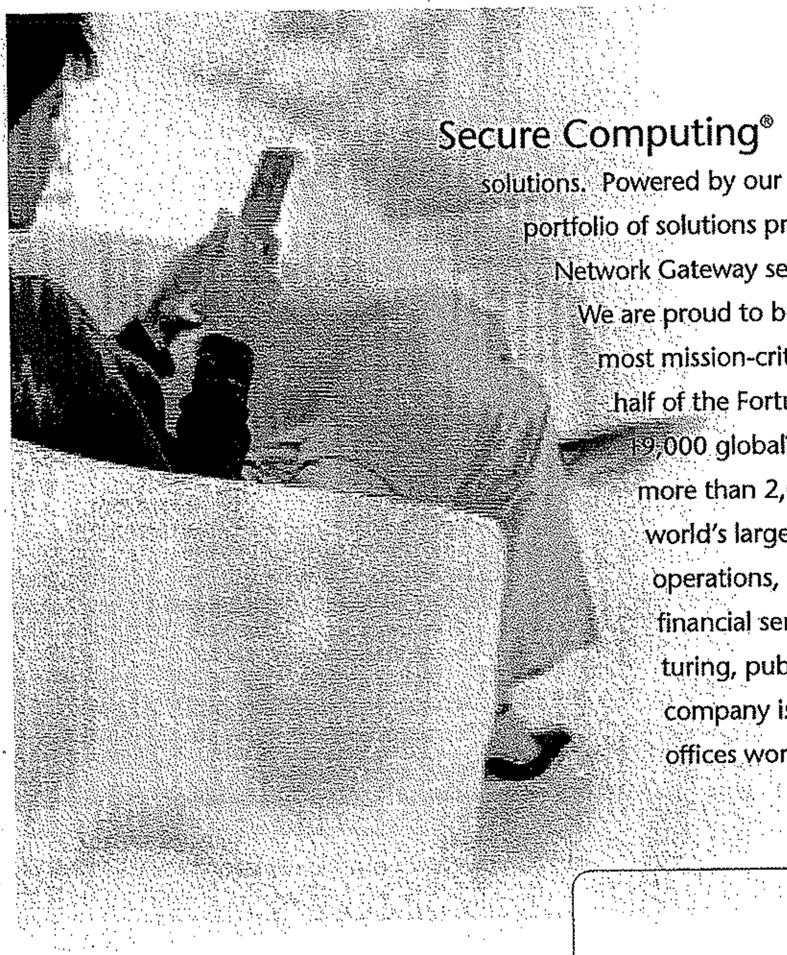
EXHIBIT 23

PART 1



Joint Trial Exhibit
JTX-45
Case No. 06-369 GMS

Annual Report 2006



Secure Computing® is a leading provider of enterprise gateway security solutions. Powered by our TrustedSource® technology, our best-of-breed portfolio of solutions provides Web Gateway, Messaging Gateway, and Network Gateway security, as well as Identity and Access Management. We are proud to be the security solutions provider to many of the most mission-critical and sensitive environments in the world. Over half of the Fortune 50 and Fortune 500 are part of our more than 19,000 global customers, supported by a worldwide network of more than 2,000 partners. Our customers operate some of the world's largest and most sophisticated electronic business operations, and include prominent organizations in banking, financial services, telecommunications, healthcare, manufacturing, public utilities, and federal and local governments. The company is headquartered in San Jose, California, and has offices worldwide.

Year Ended December 31
(Table in thousands, except per share amounts)

	2006	2005	2004	2003	2002
STATEMENT OF OPERATIONS DATA:					
Revenue	$176,697	$109,175	$93,378	$76,213	$61,960
Gross profit	127,539	87,126	75,991	63,578	51,654
Net (loss) income from continuing operations	(27,398)	21,374	12,835	9,290	(5,166)
Net (loss) income	(27,398)	21,374	12,835	8,256	(6,476)
Net (loss) income applicable to common shareholders	(43,551)	21,374	12,835	8,256	(6,476)
Diluted (loss) income per share:					
Continuing operations	(0.76)	0.57	0.34	0.28	(0.18)
Discontinued operations	—	—	—	(0.03)	(0.04)
Diluted (loss) income per share	$(0.76)	$0.57	$0.34	$0.25	$(0.22)
BALANCE SHEET DATA:					
Total assets[1]	724,128	171,763	130,914	108,475	60,943
Debt, net of fees	85,023	—	—	—	—
Convertible preferred stock	65,558	—	—	—	—
Stockholders' equity	409,741	121,883	91,826	72,014	29,663

[1] Total assets include goodwill from acquisitions of $533.7 million for 2006, $25.4 million for 2005, $25.5 million for 2004, $26.5 million for 2003 and $15.2 million for 2002.

To Our Stockholders,

2006 was an exciting and momentous year for Secure Computing, and sets a new course for our company. During the year, we completed and successfully integrated two significant acquisitions that added to our existing technology, providing a very strong foundation for our company. We also introduced several new industry-leading products to the market.

With the integration of CyberGuard and CipherTrust complete, the size, scope, and reach of our company has changed dramatically. We have become one of the largest independent security companies, and the industry leader in the Secure Content Management Appliance and Messaging Security Appliance markets. Our global footprint now encompasses over 19,000 customers in 106 countries, with over 2,000 resellers.

Equally important, through the CyberGuard and CipherTrust transactions we realized our goal of providing a comprehensive and integrated set of enterprise gateway security solutions powered by proactive protection. We have seen this need in the market develop over the last few years, and have methodically been taking the appropriate steps to either build, acquire or partner to obtain key technologies to meet the market's growing needs.

Combining three sizable organizations into one company is a major undertaking that requires dedication, planning and hard work. That undertaking is now paying off for our company, and today Secure Computing is very well positioned in the changing competitive landscape of the IT security industry. Together, we are now one company with the singular focus, of providing our customers with the products necessary to *proactively protect* their IT infrastructure at the Enterprise Gateway.

2006 Financial Performance

Despite a disappointing first half, we achieved very solid financial results in 2006. Billings were a record $219.1 million, which is an 81 percent increase compared to the prior year. Throughout 2006, we experienced strong gross margins and remained intensely focused on controlling our operating expenses.

Our company also continued its tradition of strong cash generation. In 2006, we generated a record $36.1 million of cash from operations, and used $95 million for the CipherTrust transaction. Concurrent with the closing of the transaction, we closed a senior secured debt facility that comprised of a $90 million term loan and a $20 million revolving credit facility. We ended the year with $8.7 million in cash and investments.

Addressing Today's Evolving Security Threats

Even in the earliest days of the Internet, there was a need for security. Back in those days, installing a firewall and deploying an intrusion detection system were adequate steps to control unwanted traffic. Over time, Internet use has changed dramatically and correspondingly, new threats such as spam, phishing, data leakage, and malware have emerged.

Today's Internet threat environment continues to evolve and is now populated by lower profile, targeted attacks as cyber criminals identify new ways to steal information. The attack activity has also shifted away from notoriety to financial gain. A recent FBI survey noted that computer-based attacks, launched from 36 countries, cost American businesses a staggering $67 billion in 2005.

We view demand in the security market remaining very strong. As Chief Information Officers and Chief Security Officers wrestle with today's highly sophisticated and well orchestrated attacks, we believe they are responding and will continue to respond very well to our best-of-breed, integrated capabilities at the enterprise gateway. Our products proactively protect all key access points into a company's internal network – the network gateway, the web gateway, and the messaging gateway, as well as Identity and Access Management (IAM).

The New Secure Computing

So, who is the new Secure Computing? We are a leading provider of enterprise gateway security, and address some of the fastest growing segments of our industry. Our strategy is to provide our customers with an integrated, best-of-breed product portfolio that protects the core areas of the enterprise gateway. We provide bi-directional protection by proactively blocking inbound threats such as spam, viruses, intrusion, zombies and phishing attacks, as well as guarding corporate information from data leaks and compliance violations.

Our solutions are comprehensive and centrally managed security appliances that provide real-time proactive protection powered by TrustedSource™, our global, real-time reputation system for the Internet. TrustedSource operates similarly to a credit agency monitoring past and future fiscal responsibility in the financial world. By TrustedSource monitoring and assigning a "reputation score" to a huge portion of Internet connected devices and clients based on past behavior, our suite of Enterprise Gateway Security appliances can decide if certain Internet traffic should be allowed to enter the Enterprise network. Not only does TrustedSource stop harmful email, web or application traffic at the network edge, it saves companies money by lowering bandwidth requirements and reducing the number of downstream servers.

Continued Product Innovation

Clearly, our success will be determined by our ability to understand how the industry will evolve and deliver innovative, industry-leading solutions to the market.

As part of Secure Computing's vision to provide comprehensive enterprise gateway security, earlier this year we introduced Sidewinder® 7.0 and Webwasher® 6.5. Sidewinder 7.0 is the industry's first and only firewall to incorporate reputation technology to provide proactive and reliable protection. In addition to the integration of the TrustedSource reputation technology, Sidewinder 7.0 also includes significant enhancements from CyberGuard's TSP and Classic firewall products, providing a natural and attractive upgrade path to those customers. Webwasher 6.5 is the industry's first and only reputation-based Web gateway security solution, and delivers reputation-based URL filtering for corporate users surfing the Web, and provides bi-directional protection to stop inbound threats such as spyware, phishing or other malware, and prevent outbound threats related to sensitive data leaks.

In 2007, we will be integrating our powerful TrustedSource reputation solution into key components of the IAM product suite. Strong authentication is a key component of any good enterprise security defense, and when coupled with the capabilities of reputation-based security systems, it provides significantly great defense capabilities. By adding TrustedSource into our product mix, Secure Computing will continue to increase our product superiority and differentiation with a unique additional tier of user reputation to existing IAM capabilities.

Looking ahead, we will continue to drive product innovation to ensure that we stay ahead of our competitors as well as the spammers, hackers and phishers. Secure Computing exited 2006 with 269 people in R&D, representing one of the largest research and development teams focused solely on security in the industry.

Delivering on the Promise

In 2006, we made evolutionary changes that support our long-term strategy. Now, we are fully focused on execution across all areas of our company, and delivering on the promise – to become the undisputed leader in enterprise gateway security. We believe our unique balance of financial strength, product leadership and global presence will truly position Secure Computing as a clear leader in our industry in the future.

On behalf of the Board of Directors, I would like to thank our customers, partners, employees and stockholders for your continued confidence and support.

Sincerely,

John McNulty
Chairman of the Board, President, and Chief Executive Officer

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934**

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2006

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGE ACT OF 1934**

For The Transition Period From To

Commission file number 0-27074

SECURE COMPUTING CORPORATION

(Exact name of registrant as specified in its charter)

Delaware **(State or other jurisdiction of incorporation or organization)**	**52-1637226** **(I.R.S. Employer Identification No.)**
4810 Harwood Road, **San Jose, California** **(Address of principal executive offices)**	**95124** **(Zip code)**

Registrant's telephone number, including area code: (408) 979-6100

Securities registered pursuant to Section 12(b) of the Act: None
Securities registered pursuant to Section 12(g) of the Act:
Common Stock, par value $.01 per share

Indicate by check mark if the Registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☒

Indicate by check mark if the Registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the Registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the Registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of Registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☒

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definition of "accelerated filer and large accelerated filer" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerate filer ☐ Accelerated filer ☒ Non-accelerated filer ☐

Indicate by check mark whether the Registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of the Common Stock held by non-affiliates of the Registrant as of June 30, 2006 was $426,485,662 based on the closing sale price for the Company's Common Stock on that date. For purposes of determining this number, all officers and directors of the Registrant are considered to be affiliates of the Registrant, as well as individual stockholders holding more than 10% of the Registrant's outstanding Common Stock. This number is provided only for the purpose of this report on Form 10-K and does not represent an admission by either the Registrant or any such person as to the status of such person.

As of March 12, 2007, the Registrant had 65,466,498 shares of Common Stock issued and outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's Proxy Statement for its Annual Meeting of Stockholders to be held May 10, 2007 for the year ended December 31, 2006 are incorporated by reference in Part III hereof.

TABLE OF CONTENTS

PART I

PART II

PART III

PART IV

PART I

Forward-looking statements made in this Annual Report on Form 10-K or in the documents incorporated by reference herein that are not statements of historical fact are forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. The words "expect," "plan," "anticipate," "believe," "predict," and other similar expressions identify forward-looking statements. In addition, statements which refer to projections of our future financial performance, anticipated growth and trends in our business and other discussions of future events or circumstances are forward-looking statements. A number of risks and uncertainties, including those discussed in Item 1A under the caption "Risk Factors" in this Form 10-K and the documents incorporated by reference herein, could affect such forward-looking statements and could cause actual results to differ materially from the statements made. We do not undertake any obligation to update or correct any forward-looking statements.

In this Annual Report on Form 10-K, "Secure Computing," "we," "us," "our," and "Registrant" refer to Secure Computing Corporation.

ITEM 1. BUSINESS

We are a leading provider of enterprise gateway security solutions. Our best-of-breed portfolio of solutions provide Web Gateway, Messaging Gateway, and Network Gateway Security, as well as Identity and Access Management that are further differentiated by the proactive protection provided by TrustedSource™ (global intelligence). We are proud to be the security solutions provider to many of the most mission-critical and sensitive environments in the world. Our customers operate some of the world's largest and most sophisticated electronic business operations, and include prominent organizations in banking, financial services, telecommunications, healthcare, manufacturing, public utilities, and federal, state and local governments.

Across virtually all industries, organizations are using both the Internet and corporate private intranets and extranets to expand their business. This includes inbound access for remote employees, partners, and customers, as well as employees reaching beyond the edge of the internal network to communicate and gather information across the Internet. Our commitment is to support this method for exchanging information by mitigating risks and protecting information assets from the multitude of threats present on the Internet.

The bi-directional aspect of internet protocol (IP) based information exchange and application use creates a significant challenge for enterprises in terms of protection from malware, compliance with regulatory requirements, preventing data leakage, lost productivity, and the like. Given the sophistication of network and application-layer attacks, intelligence must be shared and leveraged across security applications. This intelligence must reflect, in *real time,* the changing security profile of the Internet, and flexible mechanisms to ensure regulatory compliance and reporting need to be hard-wired into the security infrastructure. We believe layered security or "defense-in-depth" needs to be viewed not only as a best practice for perimeter defense but also as something to be extended to mission-critical applications within the network. We define and implement a comprehensive set of gateway functions required to provide this necessary defense-in-depth for the primary mission-critical applications in the enterprise. This ongoing objective is at the heart of our mission.

We have formed partnerships with a number of companies in several different capacities. We make these solutions available to customers through the best and most advantageous channels possible, including solution providers, systems integrators, distributors, and companies who include our solutions in their product offerings. These companies include, for example: Alternative Technologies, AT&T, Blue Coat Systems, Cisco, Computer Associates, Comstor, Crossbeam, Dell, EDS, F5, Hewlett-Packard, McAfee, Microsoft, Network Appliance, NetOne Systems, Novell, PGP Corporation, SafeNet, Sun PS, SAIC, Tech Data, Voltage Security, Westcon, and Workshare.

We operate our business within one operating segment called enterprise gateway security. For information regarding our revenue by geographical area, see Note 15 of the Notes to Consolidated Financial Statements. For information regarding the percentage of our revenue contributed by each of our product lines, see Item 7, *Management's Discussion and Analysis of Financial Condition and Results of Operations.*

Founded in 1989, we are incorporated in Delaware. Our principal executive offices are located at 4810 Harwood Road, San Jose, California 95124. Our telephone number at that location is (408) 979-6100. Our home page on the Internet is *www.securecomputing.com*. Other than the information expressly set forth in this annual report, the information contained, or referred to, on our website is not part of this annual report.

Acquisitions

On January 11, 2006, we completed our acquisition of CyberGuard Corporation, a leading provider of network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication, in a stock and cash transaction valued at $310.7 million. This acquisition strengthens our position as one of the market leaders in Network Gateway Security appliances, and strengthens our position in the Web Gateway Security space. CyberGuard was a logical fit for us, enhancing our strategic vision and better positioning us in two rapidly growing segments of the security industry. Along with an expanded customer and partner base, this merger provided us with important competitive advantages in the Network and Web Gateway Security markets.

On August 31, 2006, we completed our acquisition of CipherTrust, Inc., the global leader in the messaging security market, in a stock and cash transaction valued at $270.1 million. CipherTrust's products provide innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. CipherTrust's products include IronMail®, powered by TrustedSource™, IronIM™, Secure Computing Edge™, IronNet™, and RADAR™. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and messaging gateway security needs.

Industry Background

The rapid adoption of the Internet as a worldwide networking standard has accelerated the distribution and sharing of data and applications, enabling enterprises to adopt new electronic ways of doing business. The developing reliance on worldwide connectivity has allowed companies to greatly expand their business opportunities. Activities such as electronic trading of goods and services, online delivery of digital content, electronic funds transfers and share trading are now achieved in unprecedented ways. But with this growing opportunity comes new challenges for securing IT systems. The very features that give electronic business its power have elevated information security to a critical business issue.

Today's enterprise is no longer confined to a set of physical buildings; rather, the enterprise has become virtual. The Internet's power of connectivity has erased physical barriers, allowing an organization to establish ties around the globe. A business is no longer a single, isolated entity; it is part of a greater whole of interdependent entities whose lifeblood depends on the secure, electronic sharing of information. Organizations must now transcend the physical barriers of yesterday and expand their security measures *outward* to protect their digital resources beyond their physical buildings. They must also migrate their security measures *inward* to each individual's computer or laptop.

Conducting Business Over Public Networks

As Internet-based infrastructure broadens, so do the risks associated with this exposure. These risks increase daily and threaten confidentiality, integrity, and secure availability of intellectual property, proprietary data, and computing resources. Such threats present themselves in many forms, including the following:

- Malicious attacks are becoming more sophisticated and continuing to increase in volume. According to International Data Corporation (IDC), a global provider of market research, malicious code, spyware and spam continue to be the most serious threats facing corporations today, but protecting sensitive data from leaving the organization is rapidly climbing the priority list of enterprise security threats.
- Hackers and attackers are no longer focused on hobby, but rather strict and prosperous financial gain, fraud and identity theft, which continue to be the leading drivers behind the increasing sophistication and volume of attacks.
- Web-based malware programs sent on infected pages or through email downloaded from Web-based mailbox or via embedded images can attack automatically and in real time, making Web security concerns a top priority for organizations seeking protection from the jump in spyware, Trojans, worms, and other Web-traffic attacks.
- Risks from exposure to malicious software, worms, and viruses that can enter networks from many sources and cause damage, install spyware, or open secret backdoors into private computing resources.
- Theft by both infiltrators and employees of private citizen records and other proprietary information in violation of numerous federal regulations and statutes and state and local statutes, such as Sarbanes-Oxley, the Gramm-Leach Bliley Act, and the Health Insurance Portability and Accountability Act.
- Intruders gaining unauthorized access to private computing resources and software applications.
- Legal liability exposure resulting from employee Internet access, or from hijacked use of desktop personal computers and servers for unauthorized file storage and file-sharing schemes.
- Identity theft and spoofing.
- Network and application server downtime due to denial of service (DoS) and distributed denial of service attacks (DDoS).
- Confidentiality leaks via email, instant messaging chat sessions, person to person file sharing, and unauthorized attachments that leave private networks unfiltered.
- Productivity losses from spam clogged email inboxes.

Application-Level Vulnerabilities

In today's highly complex Internet environment, network attacks have evolved into application-level attacks, and recently, an entirely new class of application-specific threats have arisen that require far more stringent protection. Protecting the network is highly important, but by itself, is not sufficient. The network is the foundation for communication, and the conduit over which people connect to the application resources they need and it is precisely these applications that can expose an organization's information resources to extreme vulnerability. Our products are designed to proactively address most, if not all, network security issues, whether its employees utilizing the Internet, or remote partners and customers accessing the intranet, Web services, and applications from outside the internal network. Our security measures extend beyond the network level, protecting applications and their resources so organizations can conduct their business, expand their reach, and drive success with confidence.

From email applications to Web services, File Transfer Protocol (FTP), customer relationship management (CRM) and sales force automation systems, people connect across networks to applications in order to conduct business every day. Misuse of applications and Web portals can result in the loss of valuable resources and millions of dollars. As the applications we use have become more sophisticated, so have the attack capabilities that threaten them. Applications contain inherent vulnerabilities, and sophisticated attackers can exploit these vulnerabilities and undermine an organizations' ability to conduct its business. Defensive measures must be even *more* sophisticated in their ability to protect against application-level threats—and our technology is designed with this in mind.

Along with protecting against known threats, today's security solutions must be able to anticipate unknown threats before they enter the network. A central part of an organization's business model must include provisions for safeguarding their business connections from being compromised to the highest degree possible.

Market Need and Strategy

More than ever before, organizations realize that they must take responsibility to protect their own confidential information and that of their customers and partners. Government regulations in recent years, such as the Federal Information Security Management Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach Bliley Act, and the Children's Internet Protection Act, have heightened awareness and mandated that organizations secure their information across multiple segments—financial, medical, educational, and more. Enterprises must know that the data residing on a given network is secure and that parameters are in place for managing access to their proprietary information. Even as deadlines are met on these laws, enterprises must continue to refine their compliance solutions and move towards focusing on ongoing compliance. In the coming years, larger enterprises which had to put in a "quick fix" to meet deadlines will be looking to implement longer-term and more efficient solutions. Smaller businesses, which enjoyed some extended deadlines from Congress, are still implementing their first-time compliance solutions, representing a significant opportunity for security companies with a broad range of solutions.

Our strategy is to provide organizations, both at the enterprise level as well as the Small and Medium Business (SMB) level, with a broad set of solutions when it comes to implementing their security objectives, beginning with knowledge about security risks and regulations, accompanied by industry-leading security products to assist with mitigating these risks, and lastly, providing comprehensive security management capabilities. Our goal is to help organizations build confidence in the overall functionality and security of their network and application operations. We accomplish this by providing scalable, manageable, highly available solutions that meet their needs today and in the future. This objective includes meeting our customers' requirements for security products that provide broad solutions by integrating with each other and interoperate within current infrastructures. All of our products are designed to provide the strongest network protection available, along with central manageability, scalability, and interoperability.

Providing solutions that are manageable, easy to use and that lead the industry in total cost of ownership for the customer are our top objectives for organizations of all sizes. Our solutions enable best business practices that keep the workplace secure, productive, and easily manageable.

Our strategy also encompasses our award-winning service and support organization. We are able to provide our customers with unwavering service and support due, in part, to the knowledge base and technological expertise of our service and support staff.

Secure Computing Solutions

Our specialized solutions are designed to meet customers' needs to balance security and accessibility, and to help them create trusted environments both inside and outside their organizations. Each of our products provide a complete solution in and of itself, and they also integrate with each other for a more comprehensive, unified, and centrally managed solution. We have developed a vision for comprehensive security on the enterprise gateway that embodies the following core design principles:

- **Appliance-based delivery.** All security functionality related to application intelligence and awareness needs to reside on a contained appliance. These appliances must be built on a secure operating system platform, have a regulated set of interfaces to external systems, and be encased in strong, tamper-proof hardware. Essentially, the appliance must mitigate the many security management problems of deploying software on a standard operating system-server configuration.
- **Application and content awareness.** Today's security attacks have progressed far beyond the network and protocol level to that of the application and content. The gateway needs a deep knowledge of the underlying communication, an understanding of the context of the communication, and the ability to inspect and interpret the content.
- **Centralized policy, management and reporting.** The security gateway must have the ability to be centrally configured, provisioned and managed. This, along with consolidated reporting, should provide immediate feedback on the effectiveness of the security appliance while helping reduce the cost of ownership.
- **Bi-directional protection.** The security gateway needs to effectively scrutinize inbound traffic in order to block bad traffic from entering the network, while simultaneously performing deep inspection of outbound content to protect against leaks of confidential information or intellectual property.
- **Proactive protection.** With the rapid increase in polymorphic threats, the ability to know immediately what could be dangerous is imperative. A gateway security system should be able to effectively thwart these attacks in real time.
- **User management and education.** The security gateway needs to protect all types of sensitive data automatically, with easy-to-manage policies, comprehensive audit trails, and employee feedback loops.
- **Performance.** As traffic volumes increase exponentially, the gateways must be able to keep up and scale for performance without having to replace them, or take them off-line for major upgrades.
- **Resiliency.** Security gateways should not introduce points of failure to the mission at hand.

Our solutions for securing critical connections fall into four categories: TrustedSource Global Intelligence, enterprise gateway security appliances (Network, Web, and Messaging Gateways), Identity and Access Management, and Security and Support services.

TrustedSource Global Intelligence

We believe TrustedSource technology is the most precise and comprehensive Internet host reputation system in the world, which we are rolling into many of our product lines as a key cornerstone of Global Intelligence security. TrustedSource characterizes Internet traffic and makes it understandable and actionable, and also creates a profile of all "sender" behavior on the Internet and then utilizes this profile to watch for deviations from expected behavior for any given sender. TrustedSource then calculates a "reputation score" based on the behavior of the sending host. We have an extensive network of thousands of sensors and other collection vehicles throughout the Internet which tracks and reports back to TrustedSource, data on all observed email traffic, giving TrustedSource a real-time view of Internet communication worldwide.

Originally developed to identify spammers, TrustedSource is able to recognize any "host" profile anomalies and immediately calculate new reputation scores for senders and propagate this information to all TrustedSource clients. Analyzing not only email senders but Internet domains as well, this Global Intelligence technology is able to profile literally millions of entities connected to the Internet worldwide in real-time, and provide up-to-the minute host behavior analysis. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists and network characteristics with the unparalleled strength of our global network. We believe the result is the most complete reputation system in the industry with the ability to score every IP address across the Internet.

Enterprise Gateway Security Appliances

Network Gateway Security

Our enterprise gateway security platforms are the aggregation points not only for application-specific defense-in-depth technologies based on deep knowledge of the underlying protocols and application environment, but also a mechanism for introducing real-time intelligence to security-relevant decisions about the disposition of application-specific traffic. This incorporates host and domain intelligence as well as bi-directional security services in the areas of compliance, policy, encryption, email, Web, and anti-malware protection. These services leverage centralized policy and management and are fully integrated with TrustedSource and SafeWord® Identity and Access Management technology.

The idea of the network perimeter has evolved significantly since the advent of the Web. A mobile workforce, extranets, distributed applications and an environment of highly sophisticated, blended threats has forced enterprises to deploy an array of separate security applications to provide services such as firewall, Virtual Private Network (VPN), Intrusion-Detection System (IDS)/Intrusion-Prevention System (IPS), anti-virus, anti-spam, and more. The recent movement toward all-in-one appliances has helped mitigate the problem to an extent, especially for small and mid-size companies, but three major issues still remain: 1) many solutions rely on known malware signatures and fail to offer protection against previously unknown attacks 2) the Internet is a dynamic environment, with a security profile that changes in real time, and 3) enterprise security applications often fail to adequately share policy and application intelligence between one another. Our Network Gateway Security products address each of these areas of concern, providing the industry's strongest application firewall protections.

Sidewinder G2 Security Appliance—Our security appliances consolidate all major Internet security functions into a single system. Sidewinder G2® defends the network against all types of threats, both known and unknown. Through its unified threat management (UTM) approach, Sidewinder delivers best-of-breed anti-spyware, anti-virus, anti-spam and anti-fraud engines, Web content filtering, TrustedSource IP reputation services, secure Domain Name System (DNS), VPN, and Secure Sockets Layer (SSL) gateways, and more.

In 2006, we continued to differentiate our UTM appliance from the competition with demonstrable zero-hour attack protections on high profile Internet attacks (such as the Sendmail vulnerability in March and Microsoft Windows MetaFile "WMF" attack in January). We also announced plans to merge our newly-acquired CyberGuard® Firewall/VPN technologies (TSP and Classic) with our Sidewinder G2 Security Appliance in our next generation UTM appliance that has come to market in the first quarter of 2007. The CyberGuard acquisition also brought to us a new paradigm in enterprise central management with the Command Center which we will continue to leverage going forward. We believe Command Center's ability to do administration, configuration, monitoring, and management of software updates for a global appliance deployment coupled with our Security Reporter product's central reporting, and full out-of-the box compliance reports, continue to ensure that both medium and large customers see our network gateway appliances as the product of choice.

Sidewinder G2 continues its proven security track record, in great part due to our SecureOS® operating system with our patented Type Enforcement® technology and flexible application level protection mechanisms. In 2006, our accomplishments of FIPS 140-2 validation and continued leadership with Common Criteria (CC) EAL4+ certification for application level firewalls puts us in an unparalleled class of product when competing in the U.S. and other government opportunities all around the world.

CyberGuard Total Stream Protection (TSP)—Like Sidewinder G2, CyberGuard Total Stream Protection (TSP) line of UTM appliances is designed to protect mid-size to large enterprises against both known and zero-hour attacks, using a hybrid architecture that combines stateful packet filtering, seven layer inspection, and secure content policy enforcement. The devices include a fully integrated IPSec VPN, flexible authentication and advanced filtering strategies. Sidewinder G2 and TSP share common hardware.

SnapGear—SnapGear™ security appliances integrate networking, firewall, intrusion prevention security, and remote access requirements into one small form-factor appliance, fulfilling the lower end of the pricing scale of our network gateway security line of products. Designed to provide a complete office-in-a-box networking device for small and mid-sized organizations, SnapGear is the only networking device needed for office PCs to be networked with one another, connect securely to the Internet, connect to the corporate WAN, and service all remote access VPN needs, thereby providing small and midsize businesses with enterprise-level networking capabilities.

Web Gateway Security

Web Gateway Security appliances protect enterprises from malware, data leakage, and Internet misuse, while helping to ensure policy enforcement, regulatory compliance, and a productive application environment. These platforms analyze traffic bi-directionally. Inbound, they isolate and eliminate threats from all types of malware, including zero-day threats, viruses, Trojans, spam, phishing, and the like. They use a deep knowledge of the underlying protocols and application behavior combined with global intelligence to make security decisions. On the outbound side, in addition to preventing virus propagation and unwanted Web site access, our enterprise Web Gateway Security helps customers achieve regulatory compliance and prevent data leakage across both Web and messaging applications.

Webwasher—Webwasher® Web Gateway Security appliances provide best-of-breed content security to secure Web-based enterprise traffic. Webwasher provides URL filtering to block access to inappropriate Web content and help prevent phishing attacks, and provide malware protection with Proactive Security technology to guard against zero-day attacks and blended threats. Webwasher also features SSL Scanning which identifies and blocks malicious content hidden in SSL-encrypted traffic from accessing the network and confidential information from leaving the network. All products can be managed from a single Web Graphical User Interface (GUI) and Content Reporter offers enterprise-class reporting on all Webwasher products and most gateway cache appliances and firewalls. In 2006, and continuing into 2007, WebWasher has begun integration, and will continue, to integrate SmartFilter for its current and future URL filtering capabilities.

SmartFilter—Our flagship URL filtering application, SmartFilter®, is an enterprise solution currently shielding thousands of organizations from inappropriate use of the Web and the security threats often associated with viewing inappropriate, malicious or infected Web sites. SmartFilter provides deployment and platform flexibility with over 30 different options including leading firewalls, security appliances, proxy servers or caching systems. SmartFilter continues to be the de facto filtering standard for original equipment manufacturers (OEM). SmartFilter is integrated on market-leading solutions from vendors such as McAfee and Computer Associates.

Messaging Gateway Security

Messaging has undergone a fundamental change in enterprise environments. Not too long ago, most electronic messaging was confined to applications like Microsoft Outlook and Lotus Notes. Now with the advent of Web-based mail applications like hotmail and gmail, as well as instant messaging, there are many more channels both into and out of the enterprise network. In fact, messaging is now the preferred attack vector for hackers, and spam is their weapon of choice. Hackers now employ sophisticated networks of thousands of "zombie" computers or "botnets" to send messages infected with malware, putting the enterprise at a significant disadvantage. Even more discouraging is the sharp rise in zero-day attacks, where there is no known signature that can be used to block the attack.

Furthermore, messaging now represents a bi-directional challenge. Not only are inbound threats becoming much more sophisticated and targeted, but outbound data leakage and regulatory compliance have become huge and well-publicized liabilities for enterprises. Users can easily attach confidential documents to emails and Instant Message (IM) conversations, making it trivial for sensitive information to find its way outside the network. Outbound content checking is not common practice. And even in instances where such controls are in place, where the enterprise user is communicating over an SSL-encrypted link (i.e., HTTPS), there is typically no mechanism in place to decrypt and inspect the traffic to ensure that policies are being enforced.

Recognizing that messaging is now a primary business application in most enterprises, we have implemented a strategy to comprehensively address both inbound and outbound threats and to help our customers insure compliance with federally mandated requirements for the protection of sensitive data. Our Messaging Gateway Security platforms look at traffic bi-directionally. Inbound, they proactively isolate and eliminate threats from all types of malware—zero-day threats, viruses, Trojans, spam, phishing, and the like. We use a deep knowledge of the underlying protocols and application behavior combined with real-time global intelligence to add a new dimension to security-related processing.

On the outbound side, through sophisticated fingerprinting and data profiling techniques, our Messaging Gateways are able to determine which data (either in the form of text in a message or text within an attachment) need to be blocked or flagged due to security or compliance concerns. Our Messaging Gateways can also enforce mandatory outbound encryption for certain traffic types without requiring the installation of client software on the recipient's system. We also prevent virus propagation throughout the messaging infrastructure, delivering maximum availability and security, effectiveness and global enterprise manageability across multiple messaging protocols including email, instant messaging and Webmail. This combination of easy-to-manage gateway appliances and sophisticated, centralized real-time network intelligence provides clean, efficient communications, eliminating both inbound and outbound risks.

IronMail—IronMail® provides a centrally managed, integrated, best-of-breed messaging gateway security appliance for enterprises of all types and sizes. In one integrated appliance, IronMail protects enterprise email systems from inbound (spam, viruses, phishing, and hackers) as well as from outbound threats (regulatory or corporate policy compliance violations or theft/leakage of confidential information or intellectual property). We have integrated TrustedSource IP reputation identities into our IronMail Messaging Gateway Security appliances to provide real-time behavior analysis on more than one-third of the world's enterprise messaging traffic with over 7,000 sensors located in 48 countries.

IronIM—The IronIM™ instant messaging security appliance is the first and only solution that integrates policy to secure, log, monitor, and encrypt enterprise IM communications. IronIM allows administrators to control and manage the use of public and enterprise IM from a single management platform to eliminate risks from IM-borne threats, ensure compliance with various industry and government regulations, and monitor for information leakage or other policy violations. IronIM supports multiple instant messaging networks (including AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, and corporate IM solutions including Microsoft LCS and IBM SameTime) and does not require deployment of a new IM client.

RADAR—RADAR™ protects an organization's online reputation, whether by detecting and stopping phishing scams or identifying and fixing PCs. RADAR receives a real-time stream of behavior-based intelligence from our TrustedSource global threat correlation engine to detect deviations from expected behavior for all senders and provides real-time alerting to customers.

Secure Computing Edge—Secure Computing Edge™ is a hardened appliance positioned at the perimeter of the mail system, applying TrustedSource technology to control email traffic at the network border rather than at the mail server or desktop. Edge relies on TrustedSource for information about every sender, to allow or reject email before it even reaches critical mail servers.

Identity and Access Management

One important development in enterprise security has been recognition of the need for strong authentication as a prerequisite for access to corporate network resources (either remotely or from inside the network). Strong authentication has now been coupled with a fully-functional access gateway and the ability to coordinate policies governing the extent and scope of corporate resource access by individuals. This combination of strong authentication, centralized policy management and the ability to report at a very granular level on security-relevant activity is commonly referred to as Identity and Access Management (IAM), and is fundamental to any corporate security strategy.

We expanded our SafeWord® product line in 2006, thereby providing a comprehensive Identity and Access Management portfolio that is fully integrated into our enterprise gateway security strategy and provides strong authentication and centralized policy and reporting across the entire enterprise gateway security portfolio.

Remote access to network resources is a requirement for many businesses, but verifying the identity of your remote users with strong authentication and a reliable identity management system is vital for security. Additionally, organizations are increasingly realizing the many vulnerabilities of passwords, and they require strong authentication systems that are easy to install and deploy, simple to manage, and able to grow with their needs.

Our SafeWord products meet these needs. By providing safe access to applications, data, and resources through policy-driven security initiatives, as well as positively identifying users through strong authentication, SafeWord products assure that only the right people can make connections to an organization's applications and resources. SafeWord software and SafeWord tokens offer flexibility, scalability, and ease of use, and are used by thousands of organizations and millions of end users worldwide every day.

SafeWord SecureWire—In April 2006, we broadened our presence in the authentication market into the IAM space by introducing our SafeWord SecureWire™ appliance. IDC defines the IAM market as a comprehensive set of solutions used to identify users in a system and control their access to resources within that system by associating user rights and restrictions with the established identity. SafeWord SecureWire is a new, robust technology that functions as the access, authentication, and compliance hub for the entire network. SecureWire is designed to simplify access to applications, data, and network resources by hosting and managing all external access methods on a single appliance, such as, VPNs, Citrix applications, extranets, and Webmail. SecureWire can also host and manage all internal access methods: LAN connections, wireless LANs, and even mainframes. By providing secure access management inside and outside the virtual perimeter, and by consolidating all policies on a single device, SecureWire helps enable our customers to achieve configuration compliance because only properly configured devices are allowed to access their networks.

We include SafeWord strong authentication tokens with every SecureWire shipment to allow customers to provide proof-positive identity of all users entering their network. SecureWire is also available in a wireless package, now bundled with our SnapGear wireless appliance to provide a complete wireless access management system. The access appliance also delivers a reliable mechanism to enable configuration compliance, enforcing every end-point device to adhere to corporate IT policy, including work PCs, laptops, home PCs, and workstations. SecureWire allows our customers to mandate that only properly configured, properly secured devices are granted access according to their security policy, and to ensure that system patches, anti-virus software, and firewall protection are all in place.

SafeWord PremierAccess is our leading strong authentication solution for Microsoft environments using Active Directory, providing proof-positive user identities via VPNs, Citrix applications, Outlook Web Access, Windows Domain and Terminal Services logins. SafeWord PremierAccess® offers powerful management tools with the Enterprise Solution Pack (ESP), an optional add-on package that provides advanced user management, support for a wide range of authentication form factors, advanced reporting capabilities, and rich access control functionality.

SafeWord RemoteAccess is a simple, easy-to-use strong authentication solution designed to protect VPN, RADIUS, Citrix, and Outlook Web Access connections. With tight integration and simplified management through Active Directory, and with tokens that generate new passcodes with every user login, SafeWord RemoteAccess™ lets you easily and cost-effectively eliminate the password risk. RemoteAccess is available in the following branded versions: SafeWord RemoteAccess, SafeWord RemoteAccess-Cisco compatible, SafeWord for Citrix, SafeWord for Check Point, and SafeWord for Nortel Networks.

Security and Support Services

Our services are designed to ensure that our customers make optimal use of our products when controlling access to their networks and applications. We provide a life cycle of support and services, including: Solution Planning, Solution Implementation, and Solution Support. These services are described below.

Solution Planning—Our Security Services offerings include a variety of options for rapid assessment of a company's current network architecture and evaluation of the current status of network security. We then compare this information to the company's business needs, both current and future, to help them plan a scalable and secure e-commerce solution. In addition, we offer security policy services that help customers prepare a policy and plan that transfers their security policy from paper to practice. We provide the following services: network architecture security assessment; security policy assessment and development; and product and audit configuration assessment.

Solution Implementation—Our Network Services team offers a full range of rapid-deployment integration services and training to assist our customers through implementation and integration of our products. Both the configuration process of a security system and the security products themselves, by their nature, may have an impact on several areas within a customer's network. Accordingly, we offer a complete package of product integration assistance to ensure our customers maximize network uptime and maintain productivity during the process. We provide the following services: product implementation; product audit and configuration; and product training.

As part of our Network Services training program, we provide extensive product and network training online through our Web-based classes. In addition, we offer hands-on training at our training facilities, and these classes are also available worldwide onsite for our customers and partners. These services help our customers understand basic and advanced administration rules and tools that enable partners to configure, integrate, and maintain our products as part of a comprehensive e-business solution.

Solution Support – SecureSupport®—We offer industry leading live answer support services. SecureSupport has a team of technical support engineers that provide customer support around the clock via email, the Web, or telephone. Service options are tailored for each of our enterprise gateway security products and customer requirements. Customers can select the SecureSupport option that best meets their needs. Our support center call statistics are published and posted to our corporate Web site at www.securecomputing.com.

We designed SecureSupport Online, a tool to assist our customers and channel partners with any problem they may experience with any of our products. Through this process, technical expertise is offered online through a searchable knowledge base, viewable support history, and email access. Product patches and release notes can also be downloaded.

We offer our customers the option to purchase software support and upgrade service for an annual fee. We provide software updates and technical support through this program.

Customers

Our expanded global footprint now encompasses more than 19,000 customers operating some of the largest and most sensitive networks and applications in the world. Our partners and customers include the majority of the Dow Jones Global 50 Titans and numerous organizations in the Fortune 1000, as well as banking, financial services, healthcare, real estate, telecommunications, manufacturing, public utilities, schools, and federal, state and local governments. We have relationships with the largest agencies of the U.S. government. Our customer list also includes numerous international organizations and foreign governments. Overseas, our customers are concentrated primarily in Europe, Japan, China, the Pacific Rim, and Latin America.

No customer accounted for more than 10% of our total revenue in 2006, 2005 or 2004.

Sales

We sell our products and services both directly and indirectly through domestic and international distributors, value-added resellers, major integrators, and OEMs. For 2006, sales to major end users comprised 19% of total sales, while indirect channel sales comprised 81%. Our sales organization is divided geographically into the following territories: North America; Federal; Europe, the Middle East and Africa; Asia Pacific; and Latin America.

Our market strategy promotes our PartnersFirst reseller program, a channel program through which nearly all of our global indirect business is conducted. The program reflects our commitment to a partner-focused sales model and enhances access to our products by making them available through over 2,000 resellers via leading distribution partners and streamlined processes. Our channel program makes the process of doing business with us simple, while giving partners enhanced abilities to increase revenue.

We have a U.S. federal government sales team and a General Services Administration (GSA) schedule for our products maintained by a third party, to facilitate government orders. The U.S. government is the world's largest buyer of security products and continues to be a strong market for us.

The following table summarizes our products and services revenues (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Revenues:			
Products	$115,628	$ 79,339	$67,625
Services	61,069	29,836	25,753
	$176,697	$109,175	$93,378

Marketing

We market our products to existing customers and prospects worldwide using a variety of integrated marketing programs. Our marketing team creates and implements marketing campaigns in each of our major functional market areas: corporate marketing for company and brand awareness, product marketing, and partner marketing.

By leveraging relationships with our channel partners, we generate sales leads and brand awareness through customer focused initiatives. Additionally, we work closely with industry analysts and current customers to understand the trends and needs associated with the enterprise gateway security marketplace. Our research and experience help drive key marketing initiatives including: direct marketing, Web marketing, print advertising, customer seminars, Web seminars, and trade shows. We also work closely with outside vendors to help us pre-qualify leads in order to provide our partners with well qualified prospects.

An active international public relations program ensures that we receive appropriate press coverage for our various programs and announcements as well as obtain product reviews and speaking engagements. In addition to our marketing programs, we stimulate interest and demand for our solutions through our corporate Web site, channel partner Web sites and other industry-specific Web sites, providing white papers, newsletters, and technical notes. Several of our senior technical staff contribute articles to industry periodicals as well as abstracts for presentations they provide to industry specific summits and events, further extending our ability to educate the industry about e-business security.

Competition

The market for enterprise gateway security is highly competitive and we expect competition to intensify in the future. Our products compete on the basis of quality of security, ease of installation and management, scalability, performance and flexibility. Each of our individual products competes with a different group of competitors and products. Current significant competitors for our existing products include: Check Point Software Technologies Ltd.; Cisco Systems, Inc.; Fortinet, Inc.; Juniper Networks; EMC Corporation (formerly RSA Security, Inc.); VASCO Data Security International, Inc.; SonicWall; SurfControl, plc; Blue Coat Systems, Inc.; Symantec Corporation; Postini, Inc.; Tumbleweed; IronPort Systems, Inc.; and Websense, Inc.

Seasonality

As is typical for many large software companies, a part of our business is seasonal. A slight decline in product orders is typical in the first quarter of our fiscal year when compared to product orders in the fourth quarter of the prior fiscal year. In addition, we generally receive a higher volume of orders in the last month of a quarter. We believe this seasonality primarily reflects customer spending patterns and budget cycles.

Backlog

Our backlog for products at any point in time is not significant since products are shipped upon receipt of order. We do not believe that our backlog at any particular point in time is indicative of future sales levels. The timing and volume of customer orders are difficult to forecast because our customers typically require prompt delivery of products and a majority of our sales are booked and shipped in the same quarter. In addition, sales are generally made pursuant to standard purchase orders that can be rescheduled, reduced, or canceled prior to shipment with little or no penalty.

Manufacturing

Our manufacturing operations consist primarily of light manufacturing of our software and appliance products. We use subcontractors to duplicate software media and print user documentation and product packaging for our software products. We have two different processes for manufacturing our appliances depending on the product line. We either procure computer servers from major computer manufacturers and then assemble the final software and hardware products at our facilities in St. Paul, Minnesota or we outsource all services to third party providers. The third party providers complete the hardware build per our configuration specifications, perform a final test, and then image and drop ship the product directly to our customers.

Our SafeWord product line includes a small token, available in various designs. We source these tokens through electronics assembly manufacturers located in China.

The majority of the materials used in our manufacturing operations are industry-standard parts. Typical materials required are media and media duplication services, user documentation and other printed materials, product packaging, and computer systems (computer servers, computer peripherals, memory disk drives, and storage devices).

Research and Development

Our internal engineering staff performs internal development of new products and features. For the years ended December 31, 2006, 2005, and 2004, our research and development expenses were $34.1 million, $16.8 million, and $16.1 million, respectively.

We intend to keep our products broadly compatible with industry standards, other information security products and other applications. In addition, we will introduce new products as market demand develops for such products. We design our products so that they support emerging or evolving security and content standards, such as Hypertext Transfer Protocol (HTTP), Extensible Markup Language (XML), Simple Mail Transfer Protocol (SMTP), the Public Key Cryptography Standards (PKCS), IPSec, Lightweight Directory Access Protocol (LDAP), Internet Protocol Version 6 (IPv6), Secure Sockets Layer (SSL), and others.

Patents and Proprietary Technology

We rely on patent, trademark, copyright, and trade secret laws, employee and third party nondisclosure agreements, and other methods to protect our proprietary rights. We currently hold a number of U.S. and foreign patents relating to computer security software and hardware products. We believe that our patents are broad and fundamental to information security computer products.

Our success depends, in part, upon our proprietary software and security technology. We also rely on trade secrets and proprietary expertise that we seek to protect, in part, through confidentiality agreements with employees, consultants, and other parties.

We have used, registered, and/or applied to register certain trademarks and service marks to distinguish genuine Secure Computing products, technologies and services from those of our competitors in the U.S. and in foreign countries and jurisdictions. We enforce our trademark, service mark and trade name rights in the U.S. and abroad.

Employees

As of December 31, 2006, we had 885 employees. Of these employees, 341 were involved in sales and marketing, 123 in customer support and services, 269 in research and development, 58 in production, 39 in information technology and 55 in administrative, human resources and finance. None of our employees are represented by a labor union or is subject to a collective bargaining agreement. We believe that we maintain good relations with our employees.

Executive Officers

Our executive officers and their ages as of March 12, 2007 are as follows:

EXECUTIVE OFFICERS	AGE	POSITION WITH SECURE COMPUTING CORPORATION
John E. McNulty	60	Chief Executive Officer, President and Chairman of the Board
Jay S. Chaudhry	48	Vice Chairman and Chief Strategy Officer
Timothy J. Steinkopf	45	Senior Vice President of Operations and Chief Financial Officer
Vincent M. Schiavo	49	Senior Vice President of Worldwide Sales
Michael J. Gallagher	43	Senior Vice President of Product Development
Mary K. Budge	51	Senior Vice President, Secretary and General Counsel
Dr. Paul Q. Judge	30	Chief Technology Officer
Atri Chatterjee	44	Senior Vice President of Marketing

JOHN E. MCNULTY is our Chairman, President and Chief Executive Officer. Mr. McNulty first joined us as President and Chief Operating Officer in May 1999 and assumed the positions of Chairman of the Board and Chief Executive Officer in July 1999. From 1997 until joining us, he served as Senior Vice President of Sales, Services, and Business Development at Genesys Telecommunications Laboratories. Mr. McNulty was also previously with Intel Corporation, where he held a number of positions, including Director of Marketing and Business Development for the Enterprise Server Group, which he launched.

JAY S. CHAUDHRY is our Vice Chairman and Chief Strategy Officer. Mr. Chaudhry joined us in August 2006 as a result of our acquisition of CipherTrust, Inc. which he founded in 2000 and where he served as Chief Executive Officer. Prior to that, his experience includes sales, marketing and engineering experience with IBM, NCR and Unisys Corporation, and the successful launch of several technology companies.

TIMOTHY J. STEINKOPF is our Senior Vice President of Operations and Chief Financial Officer. Mr. Steinkopf first joined us as Treasurer and Director of Investor Relations in September 2000 and assumed the positions of Vice President and Chief Financial Officer in March 2001. Mr. Steinkopf was appointed to Senior Vice President in January 2002. From 1999 until joining us, he was at Silicon Entertainment, Inc. where his last position was Chief Financial Officer and Vice President of Finance. He was the Vice President of Finance, Secretary and Treasurer at Watt/Peterson Inc. from 1991 to 1999. Prior to that, he was at Ernst & Young LLP.

VINCENT M. SCHIAVO is our Senior Vice President of Worldwide Sales. Mr. Schiavo joined us in April 2001. From 1998 until joining us, he served as President of PolyServe, Inc. Prior to that he served as Vice President of Worldwide Sales at Sonic Solutions and in various other sales management roles at Radius, Apple Computer and Data General Corporation.

MICHAEL J. GALLAGHER is our Senior Vice President of Product Development. Mr. Gallagher rejoined us as Vice President and General Manager of our Network Security Division in 1999 and assumed the position of Senior Vice President of Product Development in August 2003. From 1997 until rejoining us, he was the Vice President of Software and Systems Engineering at Datakey. In 1996 and into 1997, he was employed by us and was responsible for management of several firewall and security initiatives. Prior to that he held various software engineering and technical management positions with increasing responsibility at Unisys Corporation.

MARY K. BUDGE is our Senior Vice President, Secretary and General Counsel. Ms. Budge joined us in November 1996 as corporate counsel and was appointed Senior Vice President in February 2005. Prior to joining us, she was an attorney for Schwegman, Lundberg, Woessner & Kluth where she specialized in trademark and copyright law. Ms. Budge is a member of the Minnesota Bar Association and the American Corporate Counsel Association.

DR. PAUL Q. JUDGE is our Chief Technology Officer. Mr. Judge joined us in August 2006 as a result of our acquisition of CipherTrust, Inc., where he served as Chief Technology Officer since 2000. Prior to that, he worked with IBM and NASA.

ATRI CHATTERJEE is our Senior Vice President of Marketing. Mr. Chatterjee joined us in August 2006 as a result of our acquisition of CipherTrust, Inc., where he served as Senior Vice President of Marketing since April 2006. From September 2003 until joining CipherTrust, he co-founded Mercora and served as the Vice President of Marketing and Business Development. In 2001 and into 2003, he served as the Vice President of Marketing and Business Development for McAfee.

None of the executive officers are related to each other or to any other director of Secure Computing.

Other

Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to those reports are available, free of charge, on our website at www.securecomputing.com as soon as reasonably practicable after they are filed with the SEC.

The public may also read and copy any materials we file with the SEC at the SEC's Public Reference Room at 100 F Street, NE, Room 1580, Washington, DC 20549. The public may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. The SEC also maintains a website at www.sec.gov that contains reports, proxy and information statements, and other information regarding issuers, such as us, that file electronically with the SEC.

ITEM 1A. RISK FACTORS

The following important factors, among others, could cause actual results to differ materially from those indicated by forward-looking statements made in this Annual Report on Form 10-K and presented elsewhere by us from time to time.

We may be unable to integrate our operations successfully and realize all of the anticipated benefits of the mergers with CipherTrust and CyberGuard. Our mergers with CipherTrust and CyberGuard involve the integration of companies that previously have operated independently, which is a complex, costly and time-consuming process. The difficulties of combining the companies' operations include, among other things:

- Coordinating geographically disparate organizations, systems and facilities;
- Integrating personnel with diverse business backgrounds;
- Consolidating corporate and administrative functions;
- Consolidating research and development, and manufacturing operations;
- Coordinating sales and marketing functions;
- Retaining key employees; and
- Preserving the research and development, collaboration, distribution, marketing, promotion and other important relationships of the companies.

The process of integrating operations could cause an interruption of, or loss of momentum in, the activities of the combined company's business and the loss of key personnel. The diversion of management's attention and any delays or difficulties encountered in connection with the merger and the integration of the two companies' operations could harm the business, results of operations, financial condition or prospects of the combined company after the mergers. We believe that the operation integration of CyberGuard is essentially complete. However, as of December 31, 2006, we have only twelve months of combined operations, and we may, in the future, encounter again any or all of the difficulties in operation integration we have faced in the period since the merger with CyberGuard, particularly due to the ongoing integration of CipherTrust. We expect the integration of CipherTrust to be completed in 2007.

We have experienced operating losses in the past and may experience operating losses in the future. In 2006 we incurred operating profit of $769,000 in the quarter ended March 31, 2006 and operating losses of $2.7 million, $6.3 million, and $9.5 million in the quarters ended June 30, 2006, September 30, 2006, and December 31, 2006, respectively. In 2005 we had continuing operating profit, although we have incurred operating losses in the past. If we are unable to attain operating profits in the future, our stock price may decline, which could cause you to lose part or all of your investment.

In 2006 we were cash flow positive, however, we have experienced negative cash flow in the past and may experience negative cash flow in the future. If, at that time, sources of financing are not available, we may not have sufficient cash to satisfy working capital requirements. We believe that we have sufficient financial resources to satisfy our working capital requirements for at least the next twelve months. We may seek to sell additional equity or debt securities or obtain an additional credit facility at that time or sooner if our plans change or if we expend cash sooner than anticipated. Any additional financing may not be available in amounts or on terms acceptable to us, if at all. Our failure to obtain financing at that time could result in our insolvency and the loss to investors of their entire investment in our common stock.

If we fail to meet the borrowing requirements under our credit agreement, we may be unable to obtain necessary short-term financing and if we default on a secured loan, material assets of ours could be subject to forfeiture. We currently are party to a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank which provides us with a $90.0 million term loan facility, a $20.0 million revolving credit facility and a swingline loan sub-facility. As of December 31, 2006, we had $88.0 million of outstanding indebtedness. Of this indebtedness, approximately $28.0 million bears interest at rates that fluctuate with changes in certain prevailing interest rates. An increase in interest rates would have a negative impact on our earnings due to an increase in interest expense. As is typical for credit facilities of this sort, the credit agreement for such credit facility imposes certain restrictions on us, including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit agreement requires us to comply with certain financial covenants, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We can offer no assurances that we will be able to comply with such financial covenants when a loan is needed or continue to comply with such covenants when a loan is outstanding. If we fail to satisfy these covenants or if we are unable to meet the conditions for borrowing under our credit agreement when funds are required, we could be prevented from meeting our payment obligations, which could have a material adverse effect on our business, financial conditional and operating results.

Further, our obligations under the credit agreement are secured by substantially all of our material assets, including real and personal property, inventory, accounts, intellectual property and other intangibles. If we default under our credit agreement for any reason and are unable to cure the default pursuant to the terms of the credit agreement, our lenders could take possession of any and all of our assets in which they hold a security interest, including intellectual property, and dispose of those assets to the extent necessary to pay off our debts, which could materially harm our business.

Our significant stockholders could have significant influence over us. Warburg Pincus beneficially owns 100% of the outstanding shares of Secure Computing Series A Preferred Stock convertible into approximately 5.7 million shares or 7.0% of Secure Computing common stock on a fully diluted basis. The shares of Series A Preferred Stock are convertible into shares of our common stock at the holder's option, at a rate determined by dividing the aggregate liquidation preference of the shares of Series A Preferred Stock to be converted by $12.75. This liquidation preference, and the shares of common stock issuable upon conversion of the Series A Preferred Stock, accretes at the rate of 5% per year, compounded semi-annually over time. Subject to certain exceptions and limitations, the liquidation preference shall accrete for 54 months from the date of issuance, giving Warburg Pincus approximately 6.7 million shares, or 8.2% of our company on a fully accreted basis. Also, Warburg Pincus holds a warrant to purchase 1,000,000 shares of common stock at an initial per share exercise price of $13.85. Additionally, Warburg Pincus is entitled to nominate a member to our board of directors and the consent of the holders of the Series A Preferred Stock is required for certain corporate actions.

Jay Chaudhry, Vice Chairman of the Board and Chief Strategy Officer, beneficially owns 5,252,636 shares of Secure Computing common stock, or 6.4% of Secure Computing common stock on a fully diluted basis. Richard Scott, a member of our Board of Directors, beneficially owns 3,977,431 shares of Secure Computing common stock, or 4.9% of Secure Computing common stock on a fully diluted basis.

Accordingly, Warburg Pincus, Jay Chaudhry, and Richard Scott could significantly influence the outcome of any corporate transaction or other matter submitted to the stockholders for approval. The interests of Warburg Pincus, Jay Chaudhry, and Richard Scott may differ from the interests of other stockholders.

Holders of our Series A Preferred Stock have rights that are senior to those of our Common Stock. Holders of our Series A Preferred Stock are entitled to receive benefits not available to holders of our common stock. These benefits include, but are not limited to, the following:

- beginning July 2010, shares of Series A Preferred Stock will be entitled to receive semi-annual dividends equal to 5.0% of the Series A Preferred Stock liquidation preference per year, which dividend may be paid in cash or added to the Series A Preferred Stock liquidation preference;
- each share of Series A Preferred Stock has an initial liquidation preference of $100 and the liquidation preference accretes daily at an annual rate of 5.0%, compounded semi-annually;

- upon a change of control of our company, Warburg Pincus may elect to (i) convert the shares of Series A Preferred Stock into shares of Common Stock and receive the consideration due to the holders of Common Stock upon conversion, or (ii) cause us to redeem the Series A Preferred Stock for cash at the liquidation preference then in effect;
- if a change of control occurs within 5 years of the issuance of the Series A Preferred Stock, the liquidation preference shall be an amount equal to the liquidation preference then in effect plus a premium of (i) 15% if the change of control occurs prior to the first anniversary of the issuance of the Series A Preferred Stock, (ii) 10% if the change of control occurs after the first anniversary of the issuance of the Series A Preferred Stock but prior to the second anniversary of the issuance of the Series A Preferred Stock, (iii) 5% if the change of control occurs after the second anniversary of the issuance of the Series A Preferred Stock but prior to the fourth anniversary of the issuance of the Series A Preferred Stock or (iv) 1% if the change of control occurs after the fourth anniversary of the issuance of the Series A Preferred Stock but prior to the fifth anniversary of the issuance of the Series A Preferred Stock;
- holders of Series A Preferred Stock have rights to acquire additional shares of our capital stock or rights to purchase property in the event of certain grants, issuances or sales;
- the conversion price of the Series A Preferred Stock, which initially was $13.51 per share, is subject to customary broad-based weighted average anti-dilution adjustments and other customary adjustments upon the issuance of shares of Common Stock below the conversion price, such as the issuance of shares and options to purchase shares in the CipherTrust acquisition, which resulted in an adjustment to the conversion price of the Series A Preferred Stock to $12.75;
- the approval of holders of majority of the Series A Preferred Stock is separately required to (i) approve changes to our certificate of incorporation or bylaws that adversely affect Warburg Pincus's rights, (ii) adopt any stockholder rights plan that would dilute the economic or voting interest of Warburg Pincus, (iii) incur certain debt, distribute assets, pay dividends or repurchase securities, (iv) create or issue any equity security with rights senior to or on parity with the Series A Preferred Stock, (v) increase the size of our board of directors above nine members and (vi) take any action that adversely affects the rights, preferences and privileges of the Series A Preferred Stock; and
- for so long as Warburg Pincus and its affiliates owns at least 50% of its shares of Series A Preferred Stock, the holders of Series A Preferred Stock will have the right, voting as a separate class, to appoint one member to our board of directors.

The potential increase in sales from our relationships with various vendors of communications, security, and network management products or managed services may be reduced by requirements to provide volume price discounts and other allowances and significant costs incurred in customizing our products. Although we do not intend that such relationships be exclusive, we may be required to enter into an exclusive relationship or forego a significant sales opportunity. To the extent we become dependent on actions by such parties, we could be adversely affected if the parties fail to perform as expected. To minimize our risk, we often set minimum quotas with our customers as a condition of exclusivity.

Competition from companies producing enterprise gateway security products could reduce our sales and market share. The market for enterprise gateway security products is intensely competitive and characterized by rapid technological change. We believe that competition in this market is likely to persist and to intensify as a result of increasing demand for security products. Each of our individual products competes with a different group of competitors and products. Because the market for our products is highly competitive, it may be difficult to significantly increase our market share or our market share may actually decline.

Our customers' purchasing decisions are based heavily upon the quality of the security our products provide, the ease of installation and management, the ability to increase the numbers of individuals using our software simultaneously, and the flexibility of our software. If a competitor can offer our customers a better solution in these areas or others and we are unable to rapidly offer a competitive product, we may lose customers. Competitors with greater resources could offer new solutions rapidly and at relatively low costs which could lead to increased price pressure, reduced margins, and a loss of market share.

Many of our competitors and potential competitors have significantly greater financial, marketing, technical, and other competitive resources than we have. Our larger actual and potential competitors may be able to leverage an installed customer base and/or other existing or future enterprise-wide products, adapt more quickly to new or emerging technologies and changes in customer requirements, or devote greater resources to the promotion and sale of their products than we can. Additionally, we may lose product sales to these competitors because of their greater name recognition and reputation among potential customers.

Our future potential competitors could include developers of operating systems or hardware suppliers not currently offering competitive enterprise gateway security products, including Microsoft, Sun Microsystems, Inc., IBM, Computer Associates, and Hewlett Packard. If any of those potential competitors begins to offer enterprise-wide security systems as a component of its hardware, demand for our solutions could decrease. Ultimately, approaches other than ours may dominate the market for enterprise gateway security products.

In the future, we may also face competition from our competitors and other parties that develop or acquire enterprise gateway security products based upon approaches that we employ. There are no guarantees that our approach will dominate the market for enterprise gateway security products. While we believe that we do not compete against manufacturers of other classes of security products, such as encryption, due to the complementary functions performed by such other classes, our customers may perceive such other companies as our competitors.

Consolidation among competitors may erode our market share. Current and potential competitors have established, or may in the future establish, cooperative relationships among themselves or with third parties to increase the ability of their products to address the needs of our prospective customers. Accordingly, it is possible that new competitors or alliances may emerge and rapidly acquire significant market share. If this were to occur, it could materially and adversely affect our financial condition or results of operations.

The trend toward multi-function security solutions may result in a consolidation of the market around a smaller number of vendors that are able to provide the necessary breadth of products and services. In the event that we are unable to internally develop all of the products needed for a complete, secure e-business solution, we may need to acquire such technology or be acquired by a larger entity. However, there can be no assurance that, in the event that we are not able to internally develop all of the products needed for an enterprise-wide security solution, we will be able to acquire or merge with other entities on terms favorable to us and our stockholders.

The pricing policies of our competitors may impact the overall demand for our products and services and therefore, impacting our profitability. Some of our competitors are capable of operating at significant losses for extended periods of time, enabling them to sell their products and services at a lower price. If we do not maintain competitive pricing, the demand for our products and/or services, as well as our market share, may decline, having an adverse effect on our business. From time to time, in responding to competitive pressures we lower the price of our products and services. When this happens, if we are unable to reduce our component costs or improve operating efficiencies, our margins could be adversely affected.

Other vendors may include products similar to ours in their hardware or software and render our products obsolete. In the future, vendors of hardware and of operating systems or other software may continue to enhance their products or bundle separate products to include functions that are currently provided primarily by enterprise gateway security software. If network security functions become standard features of computer hardware or of operating system software or other software, our products may become obsolete and unmarketable, particularly if the quality of these security features is comparable to that of our products. Furthermore, even if the enterprise gateway security and/or management functions provided as standard features by hardware providers or operating systems or other software is more limited than that of our products, our customers might accept this limited functionality in lieu of purchasing additional software. Sales of our products would suffer materially if we were then unable to develop new enterprise gateway security and management products to further enhance operating systems or other software and to replace any obsolete products.

If an OEM customer reduces or delays purchases, our revenue may decline and/or our business could be adversely affected. We currently have formed relationships with several OEMs including Cisco, Blue Coat, McAfee, Computer Associates, F5 Networks, Inc. and Network Appliance. If we fail to sell to such OEMs in the quantities expected, or if any OEM terminates our relationship, this could adversely affect our reputation, the perception of our products and technology in the marketplace and the growth of our business, and your investment in our common stock may decline in value.

Technology in the enterprise gateway security market is changing rapidly, and if we fail to develop new products that are well accepted, our market share will erode. To compete successfully, we must enhance our existing products and develop and introduce new products in a timely manner. Our net sales and operating results could be materially affected if we fail to introduce new products on a timely basis. The rate of new enterprise gateway security product introductions is substantial and security products have relatively short product life cycles. Our customer requirements and preferences change rapidly. Our net sales and operating results will be materially affected if the market adopts, as industry standards, solutions other than those we employ.

Denial of our patent applications or invalidation or circumvention of our patents may weaken our ability to compete in the enterprise gateway security market. While we believe that our pending applications relate to patentable devices or concepts, there can be no assurances that any pending or future patent applications will be granted. There is also the risk that a current or future patent, regardless of whether we are an owner or a licensee of such patent, may be challenged, invalidated or circumvented. In addition, there are no assurances that the rights granted under a patent or under licensing agreements will provide competitive advantages to us.

If another party alleges that we infringe its patents or proprietary rights, we may incur substantial litigation costs. Other than a claim made by Finjan Software Ltd., we are not aware of any third party claims that we or our products have infringed a patent or other proprietary rights. However, the computer technology market is characterized by frequent and substantial intellectual property litigation. Intellectual property litigation is complex and expensive, and the outcome of such litigation is difficult to predict. In the event that a third party were to make a claim of infringement against us, we could be required to devote substantial resources and management time to the defense of such claim, which could have a material adverse effect on our business and results of operations.

Disclosure of our trade secrets or proprietary information may undermine our competitive advantages. There can be no assurances that the confidentiality agreements protecting our trade secrets and proprietary expertise will not be breached, that we will have adequate remedies for any breach, or that our trade secrets will not otherwise become known to or independently developed by competitors.

If the use of public switched networks such as the Internet does not continue to grow, our market and ability to sell our products and services may be limited. Our sales also depend upon a robust industry and infrastructure for providing access to public switched networks, such as the Internet. If the infrastructure or complementary products necessary to take these networks into viable commercial marketplaces are not developed or, if developed, these networks do not become and continue to be viable commercial marketplaces, our net sales and operating results could suffer.

Our reliance on third party manufacturers of hardware components and subassemblies that are used in our appliances and SafeWord token product lines could cause a delay in our ability to fill orders. We currently purchase the hardware components for our appliance and Safeword token product lines from several major suppliers. Delays in receiving components would harm our ability to deliver our products on a timely basis and net sales and operating results could suffer.

Our product lines are not diversified beyond providing enterprise gateway security solutions to our customers, and any drop in the demand for enterprise gateway security products would materially harm our business. Substantially all of our revenue comes from sales of enterprise gateway security products and related services. We expect this will continue for the foreseeable future. As a result, if for any reason our sales of these products and services are impeded, our net sales and operating results will be significantly reduced.

Our stock price is highly volatile, which may cause our investors to lose money and may impair our ability to raise money, if necessary. The price of our common stock, like that of many technology companies, has fluctuated widely. During 2006, our stock price ranged from a per share high of $15.29 to a low of $4.82. Fluctuation in our stock price may cause our investors to lose money and impair our ability to raise additional capital, if necessary. Factors that may affect stock price volatility include:

- Unexpected fluctuations in operating results;
- Our competitors or us announcing technological innovations or new products;
- General economic conditions and weaknesses in geographic regions of the world;
- Threat of terrorist attacks or acts of war in the U.S. or abroad;
- Developments with respect to our patents or other proprietary rights or those of our competitors;
- Our ability to successfully execute our business plan and compete in the enterprise gateway security industry;
- Relatively low trading volume;
- Product failures; and
- Analyst reports and media stories.

If our products fail to function properly or are not properly designed, our reputation may be harmed, and customers may make product liability and warranty claims against us. Our customers rely on our enterprise gateway security products to prevent unauthorized access to their networks and data transmissions. These customers include major financial institutions, defense-related government agencies protecting national security information, and other large organizations. These customers use our products to protect confidential business information with commercial value far in excess of our net worth. Therefore, if our products malfunction or are not properly designed, we could face warranty and other legal claims, which may exceed our ability to pay. We seek to reduce the risk of these losses by attempting to negotiate warranty disclaimers and liability limitation clauses in our sales agreements. However, these measures may ultimately prove ineffective in limiting our liability for damages.

In addition to any monetary liability for the failure of our products, an actual or perceived breach of network or data security at one of our customers could harm the market's perception of our products and our business. The harm could occur regardless of whether that breach is attributable to our products.

We also face the more general risk of bugs and other errors in our software. Software products often contain undetected errors or bugs when first introduced or as new versions are released, and software products or media may contain undetected viruses. Errors or bugs may also be present in software that we license from third parties and incorporate into our products. Errors, bugs, or viruses in our products may result in loss of or delay in market acceptance, recalls of hardware products incorporating the software, or loss of data. Our net sales and operating results could be materially reduced if we experience delays or difficulties with new product introductions or product enhancements.

If we lose a significant customer, we will realize smaller profits. We derive a significant portion of our revenues from a limited number of customers. For example, our top five customers made up 10% of our sales in 2006. If we lose any of these customers or if our revenues from any of these customers are reduced, and we fail to replace the customer or fail to increase sales from other customers, we will incur smaller profits.

If we fail to collect amounts due from our customers on a timely basis, our cash flow and operating results may suffer. Because the timing of our revenues is difficult to predict and our expenses are often difficult to reduce in the short run, management of our cash flow is very important to us. Like most companies, we anticipate that a portion of the amounts owed to us will never be paid. However, if our actual collection of amounts owed to us is less than we have estimated, we will have less cash to fund our operations than we anticipated, and our financial condition and operating results could be adversely affected.

In addition, collection of amounts due us from sales to international customers generally takes longer than for other sales. Therefore, if our sales to international customers increase as a percentage of our total revenue, the average number of days it takes for us to collect amounts due from our customers may increase. If there is an increase in the time required for us to collect amounts due us, we will have less cash to fund our operations than we anticipated. This in turn could adversely affect our financial condition and operating results.

We have taken and may from time to time take various forms of action to manage the amounts due us from customers and grant customer discounts in exchange for earlier payment.

Quarterly net sales and operating results depend on the volume and timing of orders received, which may be affected by large individual transactions and which sometimes are difficult to predict. Our quarterly operating results may vary significantly depending on a number of other factors, including:

- The timing of the introduction or enhancement of products by us or our competitors;
- The size, timing, and shipment of individual orders;
- Market acceptance of new products;
- Changes in our operating expenses;
- Personnel departures and new hires and the rate at which new personnel become productive;
- Mix of products sold;
- Changes in product pricing;
- Development of our direct and indirect distribution channels;
- Costs incurred when anticipated sales do not occur; and
- General economic conditions.

Sales of our products generally involve a significant commitment of capital by customers, with the attendant delays frequently associated with large capital expenditures. For these and other reasons, the sales cycle for our products is typically lengthy and subject to a number of significant risks over which we have little or no control. We are often required to ship products shortly after we receive orders, and consequently, order backlog, if any, at the beginning of any period has in the past represented only a small portion, if any, of that period's expected revenue. As a result, our product sales in any period substantially depends on orders booked and shipped in that period. We typically plan our production and inventory levels based on internal forecasts of customer demand, which are highly unpredictable and can fluctuate substantially.

If customer demand falls below anticipated levels, it could seriously harm our operating results. In addition, our operating expenses are based on anticipated revenue levels, and a high percentage of our expenses are generally fixed in the short term. Based on these factors, a small fluctuation in the timing of sales can cause operating results to vary significantly from period to period.

The Internet may become subject to increased regulation by government agencies. Due to the increasing popularity and use of the Internet, it is possible that a number of laws and regulations may be adopted with respect to the Internet, covering issues such as user privacy, pricing and characteristics, and quality of products and services. In addition, the adoption of laws or regulations may slow the growth of the Internet, which could in turn decrease the demand for our products and increase our cost of doing business or otherwise have an adverse effect on our business, operating results or financial condition.

Anti-takeover provisions in our charter documents, share rights agreement, and Delaware law could discourage a takeover or future financing. The terms of our certificate of incorporation and share rights agreement permit our Board of Directors to issue up to 2,000,000 shares of preferred stock and determine the price, rights, preferences, privileges, and restrictions, including voting rights, of those shares without any further vote or action by our stockholders.

The Board may authorize the issuance of additional preferred stock with voting or conversion rights that could materially weaken the voting power or other rights of the holders of our common stock. The issuance of preferred stock, while providing desirable flexibility in connection with possible acquisitions and other corporate purposes could make it more difficult for a third party to acquire a majority of our outstanding voting stock. Further, provisions of Delaware law, our certificate of incorporation and our bylaws, such as a classified board and limitations on the ability of stockholders to call special meetings, and provisions of our share rights agreement could delay or make more difficult a merger, tender offer, proxy contest, or other takeover attempts.

The ability to attract and retain highly qualified personnel to develop our products and manage our business is extremely important, and our failure to do so could harm our business. We believe our success depends to a large extent upon a number of key technical and management employees. We may be unable to achieve our sales and operating performance objectives unless we can attract and retain technically qualified and highly skilled engineers and sales, consulting, technical, financial, operations, marketing, and management personnel. These personnel are particularly important to our research and development efforts and, as such, we employ a large number of technical personnel holding advanced degrees and special professional certification. Competition for qualified personnel is intense, and we expect it to remain so for the foreseeable future. We may not be successful in retaining our existing key personnel and in attracting and retaining the personnel we require. Our operating results and our ability to successfully execute our business plan will be adversely affected if we fail to retain and increase our key employee population.

Our international operations subject us to risks related to doing business in foreign countries. International sales are a substantial portion of our business. Although all of our sales are payable in U.S. dollars as of December 31, 2006, several factors could make it difficult for customers from foreign countries to purchase our products and services or pay us for obligations already incurred. Such factors include:

- Severe economic decline in one of our major foreign markets; and
- Substantial decline in the exchange rate for foreign currencies with respect to the U.S. dollar.

A decline in our international sales or collections of amounts due us from customers could materially affect our operations and financial conditions. For fiscal year 2006, 39% of our total revenue came from international sales compared to 38% in 2005. A very large drop in our sales or collections of amounts due us in these specific countries as a result of recession or other economic or political disturbances would likely harm our net sales and operating results.

In addition, we face a number of general risks inherent in doing business in international markets including, among others:

- Unexpected changes in regulatory requirements;
- Tariffs and other trade barriers;
- Legal uncertainty regarding liability;
- Threat of terrorist attacks or acts of war;

- Political instability;
- Potentially greater difficulty in collecting amounts due us;
- Longer periods of time to collect amounts due us; and
- A higher rate of piracy of our products in countries with a high incidence of software piracy.

ITEM 2. PROPERTIES

We are currently headquartered in 10,895 square feet of office space in San Jose, California. We have a facility in St. Paul, Minnesota with 107,344 square feet occupied by production, research and development, customer support and administration. We have a facility in Alpharetta, Georgia with a square footage of 75,288 that is occupied by research and development, customer support and sales. We have research facilities located in Concord, California and Deerfield Beach, Florida that occupy 17,240 and 30,148 square feet, respectively. We have foreign research facilities located in Woolongabong, Australia and Paderborn, Germany that occupy 9,529 square feet and 11,006 square feet, respectively. In support of our U.S. field sales organization, we also lease 8,198 square feet of office space in Reston, Virginia, and 10,102 in Seattle, Washington. We terminated our operations at the Seattle, Washington facility during the first quarter of 2007 but expect to sublease the facility in the future. We occupy these premises under leases expiring at various times through the year 2016. We also have foreign offices in London, England; Sydney, Australia; Munich, Germany; Paris, France; Singapore; Japan; Dubai; China and Hong Kong. We believe that our facilities are adequate for our current needs.

ITEM 3. LEGAL PROCEEDINGS

On June 5, 2006, Finjan Software, Ltd. filed a complaint entitled Finjan Software, Ltd. v. Secure Computing Corporation in the United States District Court for the District of Delaware against Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG. The complaint alleges that Secure Computing and its named subsidiaries infringe U.S. Patent No. 6,092,194 ("'194 Patent") based on the manufacture, use, and sale of the Webwasher Secure Content Management suite. Secure Computing denies infringing any valid claims of the '194 Patent. The answer to the complaint was filed on July 26, 2006. Discovery is proceeding.

On January 19, 2007, Rosenbaum Capital, LLC filed a putative securities class action complaint in the United States District Court for the Northern District of California against us and certain directors and officers of the company. The alleged plaintiff class includes persons who acquired our stock between May 4, 2006 through July 11, 2006. The complaint alleges generally that defendants made false and misleading statements about our business condition and prospects for the fiscal quarter ended June 30, 2006, in violation of Section 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. The complaint seeks unspecified monetary damages. While there can be no assurance as to the outcome of this or any other litigation we believe there are meritorious legal and factual defenses to this action and we intend to defend ourselves vigorously.

ITEM 4. SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS

No matters were submitted to a vote of the stockholders during the three months ended December 31, 2006.

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information

Our common stock is listed on the NASDAQ national market under ticker symbol: SCUR. As of March 12, 2007, there were approximately 3,900 registered holders. The number of registered holders represents the number of shareholders of record plus the number of individual participants in security position listings. We believe, however, that many beneficial holders of our common stock have registered their shares in nominee or street name and that there are approximately 14,000 beneficial owners. The low and high sale price of our common stock during the last eight quarters is as follows:

	2006		2005	
Quarter	High	Low	High	Low
First	15.29	11.08	10.75	7.38
Second	11.85	7.65	11.83	8.01
Third	8.68	4.82	12.91	10.32
Fourth	7.27	6.15	14.70	10.74

We have not paid any dividends on our common stock during the periods set forth above. It is presently the policy of the Board of Directors to retain earnings for use in expanding and developing our business. Accordingly, we do not anticipate paying dividends on the common stock in the foreseeable future.

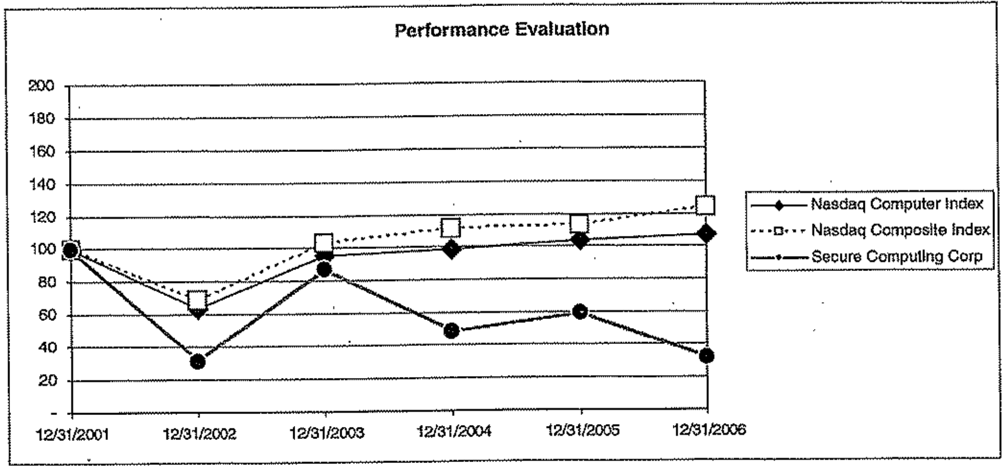
Sale of Unregistered Securities

On August 17, 2005, we entered into a Securities Purchase Agreement with Warburg Pincus IX, L.P., as amended December 9, 2005. Pursuant to the terms of the Securities Agreement, we agreed to issue to Warburg Pincus 700,000 shares of Series A Preferred Stock and a warrant to purchase 1,000,000 shares of our common stock in exchange for $70 million, subject to stockholder approval, among other conditions. The shares of Series A Preferred Stock are convertible at $12.75 a share, and include a 5% accretive dividend. The warrant is exercisable at a price of $13.85 per share. On January 11, 2006, our stockholders approved the issuance of shares of Series A Preferred Stock and a warrant to purchase shares of our common stock to Warburg Pincus, and we issued the shares of Series A Preferred Stock and the warrant on January 12, 2006. The issuance was deemed to be exempt from registration under the Securities Act of 1933 in reliance upon Section 4(2) thereof as transactions by an issuer not involving any public offering. We filed a Registration Statement on Form S-3 which registered the shares of common stock issuable upon conversion of the Series A Preferred Stock and the common stock issuable upon exercise of the warrant for resale.

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. The aggregate purchase price was $270.1 million consisting primarily of $188.1 million in cash, the issuance of 10.0 million shares of common stock valued at $68.1 million, the conversion of outstanding CipherTrust stock options into options to purchase 2.5 million shares of our common stock with a fair value of $7.8 million, and direct costs of the acquisition of $6.1 million. The issuance of 10.0 million shares of common stock was exempt from registration pursuant to Section 4(2) of the Securities Act of 1933, as amended, and pursuant to Rule 506 of Regulation D of the Securities Act.

Performance Evaluation

The graph below compares total cumulative stockholders' return on the common stock for the period from the close of the NASDAQ Stock Market—U.S. Companies on December 31, 2001 to December 31, 2006, with the total cumulative return on the Computer Index for the NASDAQ Stock Market—U.S. Companies (the "Computer Index") and the Composite Index for the NASDAQ Stock Market (the "Composite Index") over the same period. The index level for the graph and table was set to 100 on December 31, 2001 for the common stock, the Computer Index and the Composite Index and assumes the reinvestment of all dividends.



ITEM 6. SELECTED FINANCIAL DATA

The consolidated statement of operations data set forth below for the fiscal years ended December 31, 2006, 2005 and 2004, and the consolidated balance sheet data at December 31, 2006 and 2005, are derived from the audited consolidated financial statements included elsewhere in this Form 10-K. The consolidated statement of operations data set forth below for the fiscal years ended December 31, 2003 and 2002 and the consolidated balance sheet data at December 31, 2004, 2003 and 2002, are derived from audited consolidated financial statements which are not included in this Form 10-K. You should read the data set forth below in conjunction with the financial statements and notes thereto and "Management's Discussion and Analysis of Financial Condition and Results of Operations" included elsewhere in this Form 10-K.

	Year Ended December 31,				
	(Table in thousands, except per share amounts)				
	2006	2005	2004	2003	2002
STATEMENT OF OPERATIONS DATA:					
Revenue	$176,697	$109,175	$ 93,378	$ 76,213	$61,960
Gross profit	127,539	87,126	75,991	63,578	51,654
Net (loss) income from continuing operations	(27,398)	21,374	12,835	9,290	(5,166)
Net loss from discontinued operations/disposal of AT division	—	—	—	(1,034)	(1,310)
Net (loss) income	(27,398)	21,374	12,835	8,256	(6,476)
Net (loss) income applicable to common shareholders	(43,551)	21,374	12,835	8,256	(6,476)
Basic (loss) income per share:					
Continuing operations	(0.76)	0.59	0.36	0.29	(0.18)
Discontinued operations	—	—	—	(0.03)	(0.04)
Basic (loss) income per share	$ (0.76)	$ 0.59	$ 0.36	$ 0.26	$ (0.22)
Diluted (loss) income per share:					
Continuing operations	(0.76)	0.57	0.34	0.28	(0.18)
Discontinued operations	—	—	—	(0.03)	(0.04)
Diluted (loss) income per share	$ (0.76)	$ 0.57	$ 0.34	$ 0.25	$ (0.22)
BALANCE SHEET DATA:					
Total assets (1)	724,128	171,763	130,914	108,475	60,943
Debt, net of fees	85,023	—	—	—	—
Convertible preferred stock	65,558	—	—	—	—
Stockholders' equity	409,741	121,883	91,826	72,014	29,663

(1) Total assets include goodwill from acquisitions of $533.7 million for 2006, $39.2 million for 2005, $39.3 million for 2004, $40.5 million for 2003, and $15.2 million for 2002.

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

Information Regarding Forward-Looking Statements

The following discussion contains forward-looking statements, including statements regarding our expectations, beliefs, intentions, or strategies regarding the future. These statements are not guarantees of future performance and are subject to risks, uncertainties, and other factors, some of which are beyond our control and difficult to predict and could cause actual results to differ materially from those expressed or forecasted in the forward-looking statements. The risks and uncertainties are summarized in Item 1A above and in the other documents we file with the SEC. These forward-looking statements reflect our view only as of the date of this report. We cannot guarantee future results, levels of activity, performance, or achievement. We do not undertake any obligation to update or correct any forward-looking statements.

Executive Overview

We are a leading provider of enterprise gateway security solutions. Our best-of-breed portfolio of solutions provides Web Gateway, Messaging Gateway, and Network Gateway security, as well as Identity and Access Management that are further differentiated by the proactive protection provided by TrustedSource (global intelligence).

Our specialized solutions are designed to meet customers' needs to balance security and accessibility, and to help them create trusted environments both inside and outside their organizations. Each of our products provides a complete solution in and of itself, and they also integrate with each other for a more comprehensive, unified, and centrally managed solution. We have developed a vision for comprehensive security on the enterprise gateway that embodies the following core design principles: appliance-based delivery; application and content awareness; centralized policy, management and reporting; bi-directional protection; proactive protection; user management and education; performance; and resiliency.

In 2005 we embarked on a strategy to significantly increase our presence in the industry and to define and become the leader in the enterprise gateway security market. We believe that our acquisitions of CyberGuard and CipherTrust in 2006 have laid a strong foundation for our future success.

Through the CipherTrust acquisition in 2006, we acquired TrustedSource technology and entered the Messaging Gateway security market.. We believe TrustedSource technology is the most precise and comprehensive Internet host reputation system in the world, and we are rolling this system into many of our product lines as a key cornerstone of Global Intelligence security. Recognizing that messaging is now a primary business application in most enterprises, we have implemented a strategy to comprehensively address both inbound and outbound threats and to help our customers insure compliance with federally mandated requirements for the protection of sensitive data. Our Messaging Gateway Security products include IronMail, IronIM, RADAR, and Secure Computing Edge.

Also in 2006, we added the Webwasher Web Gateway security product to our Web Security Gateway product line through the CyberGuard acquisition. Web Gateway Security appliances protect enterprises from malware, data leakage, and Internet misuse, while helping to ensure policy enforcement, regulatory compliance, and a productive application environment.

This year we continued to differentiate our UTM appliance from the competition with demonstrable zero-hour attack protections on high profile Internet attacks (such as the Sendmail vulnerability in March and Microsoft Windows MetaFile "WMF" attack in January). We also announced plans to merge our newly-acquired CyberGuard Firewall/VPN technologies (TSP and Classic) with our Sidewinder G2 Security Appliance in our next generation UTM appliance that has come to market in the first quarter of 2007. The CyberGuard acquisition also brought to us a new paradigm in enterprise central management with the Command Center which we will continue to leverage going forward. We believe Command Center's ability to do administration, configuration, monitoring, and management of software updates for a global appliance deployment coupled with our Security Reporter product's central reporting, and full out-of-the box compliance reports, continue to ensure that both medium and large customers see our network gateway appliances as the product of choice.

Early in 2006 we broadened our presence in the authentication market into the IAM space by introducing our SafeWord SecureWire appliance. SafeWord SecureWire is a new, robust technology that functions as the access, authentication, and compliance hub for the entire network. By providing secure access management inside and outside the virtual perimeter, and by consolidating all policies on a single device, SecureWire helps enable our customers to achieve configuration compliance because only properly configured devices are allowed to access their networks.

Our Network Gateway Security revenue represented 53% of total revenue and an 87% or $43.3 million increase over the prior year. The acquired CyberGuard TSP and Classic product lines contributed $44.7 million.

Our Web Gateway Security revenue represented 26% of total revenue and a 46% or $14.6 million increase over the prior year. The acquired Webwasher product line contributed $18.4 million. This increase was slightly offset by a $3.5 million decline in sales of our Bess and Sentian product lines when these products were discontinued in 2006. Our Identity and Access Management revenue represented 17% of total revenue, which is a 9% increase over the prior year. This increase was driven by sustained demand for high assurance solutions. Messaging Gateway Security revenue, added through the sales of the acquired CipherTrust product line, represented 4% of total revenue for the full year 2006. Because we are unable to establish vendor specific objective evidence (VSOE) of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred and will be recognized as revenue over the term of the undelivered elements.

Our customers operate some of the largest and most sensitive networks and applications in the world. Our partners and customers include the majority of the Dow Jones Global 50 Titans and numerous organizations in the Fortune 1000, as well as banking, financial services, healthcare, telecommunications, manufacturing, public utilities, schools and federal, state and local governments. We also have close relationships with the largest agencies in the U.S. government.

International sales accounted for 39% of total revenue during 2006. Major foreign markets for our products include Europe, Japan, China, the Pacific Rim and Latin America. In each market, we have independent channel partners responsible for marketing, selling and supporting our products to resellers and end users. In 2006, our market presence continued to expand through our extensive worldwide network of value-added resellers, distributors, and OEM partners. These partners generated 81% of our sales in 2006.

Each of our individual products competes with a different group of competitors and products. In this highly competitive market, characterized by rapid technological change, our customers' purchasing decisions are based heavily upon the quality of the security our products provide, the ease of installation and management, and the scalability and flexibility of our software.

Specific challenges and risks that our product lines face include, but are not limited to: responding to competitor pricing policies and competitive features; rapid technological change in the network security market; and risk of bugs and other errors in our software.

On January 11, 2006, we completed our acquisition of CyberGuard Corporation, a leading provider of network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication, in a stock and cash transaction valued at $310.7 million. This acquisition strengthened our position as one of the market leaders in Network Gateway Security appliances, and strengthened our position in the Web Gateway Security space. CyberGuard was a logical fit for Secure Computing, enhancing our strategic vision and better positioning us in two rapidly growing segments of the security industry. Along with an expanded customer and partner base, this merger provided us with important competitive advantages in the Network and Web Gateway Security markets.

On January 12, 2006, we received from Warburg Pincus Private Equity IX, L.P., a global private equity fund, $70.0 million in proceeds from the issuance of 700,000 of Series A Convertible Preferred Stock (the preferred stock), a warrant to acquire 1.0 million shares of our common stock that vested on that date and an election of a member to our Board of Directors. Based on a quoted market price as of January 12, 2006 and the fair value of the warrant as determined using the Black-Scholes model, we valued the preferred stock at $62.0 million and the warrant at $8.0 million. The proceeds from this transaction were used to finance most of the cash portion of the CyberGuard acquisition. On August 31, 2006, the conversion price for the preferred stock was adjusted from the original price of $13.51 to $12.75 per share and the exercise price for the warrant was adjusted from the original price of $14.74 to $13.85 per share in accordance with an anti-dilution provision triggered by the CipherTrust acquisition.

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. The CipherTrust products provide innovative layered security solutions to stop inbound

EXHIBIT 23

PART 2

messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. The acquired products from CipherTrust include IronMail, powered by TrustedSource, IronIM, IronMail Edge, IronNet, and RADAR. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and Messaging Gateway security needs.

On August 31, 2006, we entered into a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank. The credit facility provided for a $90.0 million term loan facility, a $20.0 million revolving credit facility, and a swingline loan sub-facility. The proceeds from this transaction were used to finance a portion of the CipherTrust acquisition. The term loan matures on August 31, 2013 and is payable in 27 scheduled quarterly installments of $225,000 beginning in December 2006 with a final payment of $83.9 million due at maturity. Interest is payable quarterly on the term loan at the London Interbank Offered Rate ("LIBOR") + 3.25%. The interest rate on the term loan may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +3.00%.

The revolving credit facility matures on August 31, 2012 with interest payable quarterly at LIBOR + 3.25%. The interest rate on the revolving credit facilities may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +2.75%. The revolving credit facility also requires that we pay an annual commitment fee of .5%. The annual commitment fee, based on our Leverage Ratio and ranging from .5% to .375%, is payable quarterly in arrears. The Leverage Ratio is defined as the ratio of (a) consolidated indebtedness to (b) consolidated adjusted EBITDA (earnings before interest, taxes, depreciation, amortization and other adjustments as defined in the agreement). The Leverage Ratio will be calculated quarterly on a pro forma basis that includes the four preceding quarters. The initial Leverage Ratio calculation will be as of December 31, 2006 and cannot exceed the following thresholds over the term of the loan: August 31, 2006 through December 31, 2006 – 4.75 to 1.00; First six months of Fiscal 2007 – 4.00 to 1.00; Last six months of Fiscal 2007 – 3.50 to 1.00; Fiscal 2008 – 2.50 to 1.0; Fiscal 2009 – 2.25 to 1.00; Fiscal 2010 through maturity – 2.00 to 1.00.

The obligations under the senior secured credit facility are guaranteed by us and are secured by a perfected security interest in substantially all of our assets. Financing fees incurred in connection with the credit facility were deferred and are included as a reduction to our long-term debt. These fees are being amortized to interest expense over the term of the term loan using the effective interest rate method.

The credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain financial covenants, including maintaining leverage and interest coverage ratios and capital expenditure limitations.

We incurred a net loss $27.4 million in 2006 compared to net income of $21.3 million in 2005. The net loss is a result of costs not incurred in 2005, such as: share-based compensation of $10.6 million, litigation expense of $2.5 million, amortization of intangible assets of $16.5 million, additional tax expense of $8.9 million and one-time acquisition related costs and write-off of impaired fixed asset of $2.6 million. In addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates. Until we are able to establish VSOE on the sales of our CipherTrust product line and our revenue outpaces our operating expenses, including share-based compensation and amortization of intangible assets, we expect to generate net losses going forward.

As of December 31, 2006, we had $8.7 million in cash and short-term investments with no outstanding borrowings on our $20 million revolving credit facility. We generated $36.1 million in cash from operations for the year. We expect to generate cash during 2007 as we expect billings to continue to grow at a faster rate than operating expenses.

Results of Operations

The following table sets forth, for the periods indicated, the statements of operations of our company expressed as a percentage of revenue:

	Year ended December 31,		
	2006	2005	2004
Revenues:			
Products	65%	73%	72%
Services	35	27	28
Total revenues	100	100	100
Cost of revenues:			
Products	18	15	13
Services	7	5	6
Amortization of purchased intangibles	3	—	—
Total cost of revenues	28	20	19
Gross profit	72	80	81
Operating expenses:			
Selling and marketing	48	39	44
Research and development	19	15	17
General and administrative	8	7	7
Amortization of purchased intangibles	6	—	—
Litigation settlement	1	—	—
Total operating expenses	82	61	68
Operating (loss)/income	(10)	19	13
Other (expense)/income	(—)	2	1
(Loss)/income before tax	(10)	21	14
Income tax expense	(6)	(1)	—
Net (loss)/income	(16%)	20%	14%
Preferred stock accretion	(2)	—	—
Charge from beneficial conversion of preferred stock	(7)	—	—
Net (loss)/income applicable to common shareholders	(25%)	20%	14%

Comparison of Years Ended December 31, 2006 and 2005.

Revenue. Our total revenues increased 62% to $176.7 million in 2006, up from $109.2 million in 2005. Our product revenues increased 46% to $115.6 million in 2006, up from $79.3 million in 2005. Our service revenues increased 105% to $61.1 million in 2006, up from $29.8 million in 2005. The increase in total revenues in 2006 was driven by growth across all product categories. Our Network Gateway Security revenue represented 53% of total revenue and an 87% or $43.3 million increase over the prior year. The acquired CyberGuard TSP and Classic product lines contributed $44.7 million. Our Web Gateway Security revenue represented 26% of total revenue and a 46% or $14.6 million increase over the prior year. The acquired Webwasher product line contributed $18.4 million. This increase was slightly offset by a $3.5 million decline in sales of our Bess and Sentian products when these products were discontinued in 2006. Our Identity and Access Management revenue represented 17% of total revenue, which is a 9% increase over the prior year. This increase was driven by sustained demand for high assurance solutions. Messaging Gateway Security revenue, added through the sales of the acquired CipherTrust product lines and represented 4% of total revenue for the full year 2006. Because we are unable to establish VSOE of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred and will be recognized as revenue over the term of the undelivered elements.

Cost of Revenues and Gross Profit. Total cost of revenues, which includes products and services costs and the amortization of purchased intangibles, increased 124% to $49.2 million in 2006, up from $22.0 million in 2005. This increase is the direct result of the increase in total revenues and the addition of the amortization of purchased intangibles and share-based compensation. Gross profit as a percentage of revenue decreased from 80% in 2005 to 72% in 2006. Gross profit for products decreased to 68% in 2006 compared to 79% in 2005. This decline was driven by the amortization of the developed technologies acquired in the CyberGuard and CipherTrust acquisitions and by the increased sales volume on products containing a hardware component, which have a lower gross profit margin than our software products. Gross margins were also reduced as more of our business continues to be transacted with channel partners versus direct to end users. In 2006 sales to our indirect channel partners comprised 81% of total sales versus 73% of total sales in 2005. Gross profit for services was 81% in 2006 compared to 83% in 2005. The decline in the gross profit rate for services was primarily driven by increased customer support costs due to share-based compensation and increased headcount and related costs in 2006 compared to 2005.

Operating Expenses. Operating expenses consist of selling and marketing, research and development, and general and administrative expenses, amortization of purchased intangible assets, and non-recurring litigation settlement costs. Total operating expenses increased 118% to $145.3 million for 2006, up from $66.8 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions. To a lesser extent, operating expenses increased as a result of inflationary increases in payroll and related costs, and increases in allocated corporate costs. As a percentage of revenue, total operating expenses were 82% for 2006 compared to 61% in 2005. This increase was primarily driven by the inclusion of costs not incurred in 2005, such as: share-based compensation of $9.6 million, amortization of purchased intangibles of $10.6 million, litigation settlement expense of $2.5 million, and one-time costs for severance due to acquisition related restructurings, duplicate and one-time integration costs, facility move costs and the write-off of an asset that was deemed to be fully impaired as a result of our acquisition of CipherTrust of $2.6 million. In addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates.

Selling and Marketing. Selling and marketing expenses consist primarily of salaries, commissions, share-based compensation and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, public relations, travel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Our customer support function, which provides support, training and installation services, is also responsible for supporting our sales representatives and sales engineers throughout the sales cycle by providing them and our prospective customers with technical assistance and, as such, a portion of those costs are included here. Selling and marketing expenses increased 100% to $84.5 million in 2006, up from $42.3 million in 2005. This increase was driven primarily by increased headcount and related costs along with severance for restructurings as a result of the CyberGuard and CipherTrust acquisitions, and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, the write-off of an asset that was deemed fully impaired as a result of the CipherTrust acquisition and inflationary increases in allocated corporate costs. As a percentage of revenue, selling and marketing expenses were 48% in 2006 compared to 39% in 2005. This increase was driven by one-time costs for our acquisitions, share-based compensation costs, and in addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates.

Research and Development. Research and development expenses consist primarily of salaries, share-based compensation and benefits for our product development and advanced technology personnel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Research and development expenses increased 103% to $34.1 million in 2006, up from $16.8 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, and inflationary increases in allocated corporate costs. As a percentage of revenue, research and development expenses were 19% for the year compared to 15% in 2005. This increase was driven by share-based compensation costs and in addition, the acquired and assumed CyberGuard and CipherTrust expense rates were higher as a percentage of revenue than our prior year stand-alone expenses.

General and Administrative. General and administrative expenses consist primarily of salaries, share-based compensation, benefits and related expenses for our executive, finance and legal personnel, directors and officers insurance and allocations of corporate costs, which include information technology, facilities and human resources expenses. General and administrative expenses increased 89% to $13.6 million in 2006, up from $7.2 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions, legal fees, and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, audit fees, and inflationary increases in allocated corporate costs. As a percentage of revenue, general and administrative expenses were 8% in 2006 compared to 7% in 2005. This increase was primarily due to duplicate costs incurred for the transitional employees due to the acquisitions.

Amortization of Purchased Intangible Assets. Amortization of purchased intangible assets consists of the amortization of tradenames and customer lists acquired in the CipherTrust and CyberGuard acquisitions, described in Note 2 and 3 of the Notes to the Consolidated Financial Statements, respectively, and to a lesser extent the N2H2 acquisition in 2003. Amortization of these acquired tradenames and customer lists was $10.6 million, or 6% of revenue, in 2006 compared to $496,000, or less than 1% of revenue, in 2005. This increase is due to the additional intangibles acquired in the CyberGuard and CipherTrust acquisitions.

Share-Based Compensation Expense. On January 1, 2006, we adopted Statement of Financial Accounting Standards (SFAS) No. 123(R), "Share-Based Payment," which requires the measurement and recognition of compensation expense for all share-based payment awards made to employees and directors including employee stock options and employee stock purchases based on estimated fair values. Share-based compensation expense related to stock options, restricted stock and shares purchased under our ESPP under SFAS 123(R) for the year ended December 31, 2006 was allocated as follows (in thousands):

	Year Ended December 31, 2006
Cost of product revenues	$ 357
Cost of service revenues	567
Selling and marketing	5,260
Research and development	2,542
General and administrative	1,830
Total share-based compensation expense	$10,556

There was no share-based compensation expense recognized for the year ended December 31, 2005.

Litigation Settlement. Litigation settlement expense of $2.5 million pertains to a charge related to litigation brought by the landlord of our former Concord, CA office. This expense represents a judgment in favor of the plaintiff for $1.1 million and additional costs of $1.4 million we incurred related to damages. The settlement was paid in July 2006.

Other (Expense)/Income. Other expense was $120,000 in 2006 as compared to other income of $1.6 million in 2005. The decrease is primarily a result of incurred interest expense related to debt assumed for the CipherTrust acquisition and a decrease in interest income on a decreased average cash balance.

Income Taxes. During 2006, we recorded income tax expense of $9.5 million. Of this $9.5 million income tax expense, a non-cash expense of $8.5 million is related to a net tax valuation allowance recorded on our net deferred tax assets. We were unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses, and needed to provide tax expense for the subsequent valuation allowance reapplied to the remaining net operating losses. This was a result of changes in circumstances due to recent acquisitions that caused a change in judgment regarding the realizability of our net deferred tax assets in the fourth quarter. The remainder of the income tax expense is related to current income tax components such as, alternative minimum income tax, and state and foreign income taxes. This is compared with $608,000 of income tax expense recorded in 2005 which consisted of $349,000 for alternative minimum tax expense, $58,000 for state income tax expense and $201,000 for various foreign income tax expenses.

Federal alternative minimum tax was provided on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carryforward which we have available. Similar to 2006, we anticipate that we will be in an alternative minimum taxable income position in 2007. Current tax law provides that part or all of the amount of the alternative minimum tax paid can be carried forward indefinitely and credited against federal regular tax in future tax years to the extent the regular tax liability exceeds the alternative minimum tax in those years. For 2006, the reversal of $3.1 million of the tax valuation allowance related to acquired net operating losses was recorded as a decrease to goodwill in the balance sheet and not as a benefit to tax expense in the income statement.

In accordance with SFAS No. 109, we have assessed the likelihood that the net deferred tax assets will be realized. SFAS No. 109, "Accounting for Income Taxes," requires the consideration of a valuation allowance in all circumstances, if the conclusion is not more likely than not a valuation allowance is required. We have determined that it is more likely than not that deferred tax assets of $24.4 million at December 31, 2006 will be realized based on our expected future reversals of certain deferred tax liabilities. We have a net deferred tax liability recorded in our balance sheet that consists primarily of indefinite lived intangible assets that are not deductible for tax purposes and therefore cannot be used to realize additional reversing deferred tax assets. In accordance with SFAS No. 109, our remaining noncurrent deferred tax liabilities are netted with our noncurrent deferred tax assets and are presented as a single amount in our consolidated balance sheet.

Worldwide net operating loss carryforwards totaled approximately $479.5 million at December 31, 2006, comprised of $456.6 million domestic net operating loss carryforwards and $22.9 million of international net operating loss carryforwards. These carryforwards are available to offset taxable income through 2026 and will start to expire in 2011. Of these carryforwards, $208.1 million relates to acquired CyberGuard net operating losses, $59.6 million relates to acquired N2H2 net operating losses, and $19.4 million relates to acquired CipherTrust net operating losses. We have provided a complete valuation allowance on primarily all of these acquired losses are fully valued against, and upon release of the valuation allowance, a portion of the benefit will go to the balance sheet to reduce goodwill instead of a benefit to the income tax provision. As of December 31, 2006 we have deducted $56.8 million related to stock option exercises. The tax benefit in excess of book expense from these stock option exercises will be recorded as an increase to additional paid-in capital upon utilization of the net operating losses under the financial statement approach to recognizing the tax benefits associated with stock option deductions. Of the remaining benefit associated with the carryforwards, approximately $111.3 million has yet to be recognized in the consolidated statement of operations. However, there are no assurances that the tax benefit of these carryforwards will be available to offset future income tax expense when taxable income is realized.

As a matter of course, we are regularly audited by federal, state, and foreign tax authorities. From time to time, these audits result in proposed assessments. During the fourth quarter of 2006, we reached a settlement with the Internal Revenue Service regarding all assessments proposed with respect to the CipherTrust federal income tax return for 2004. The Internal Revenue Service has commenced its examination of CipherTrusts federal income tax returns for 2003 and 2005. In our opinion, the final resolution of these audits will not have a material adverse effect on our consolidated financial position, liquidity or results of operations. We anticipate the completion of these field audits during 2007.

Estimates were used in the determination of our provision for income taxes, current income taxes payable, as well as in our deferred tax asset and liability analysis. These estimates take into account current tax laws and our interpretation of these current tax laws within the various taxing jurisdictions within which we operate. Changes in the tax laws or our interpretation of tax laws and the resolution of future audits could impact our provision for income taxes.

Comparison of Years Ended December 31, 2005 and 2004.

Revenues. Our total revenues increased 17% to $109.2 million in 2005, up from $93.4 million in 2004. Our product revenues increased 17% to $79.3 million in 2005, up from $67.6 million in 2004. Our service revenues increased 16% to $29.8 million in 2005, up from $25.8 million in 2004. The increase in total revenues in 2005 was driven by growth across all product lines. Our Network Gateway Security revenue (formerly known as the Sidewinder G2 Firewall product line) increase was due to increased demand for our security appliance. Our Web Gateway Security revenue (formerly known as the Web filtering product line) increase was due to continued traction through OEM relationships. The Identity and Access Management revenue (formerly known as the SafeWord product line) increase was driven by sustained demand for high assurance solutions.

Cost of Revenues and Gross Profit. Total cost of revenues, which includes products and services costs, increased 27% to $22.0 million in 2005, up from $17.4 million in 2004. This increase is the direct result of the increase in total revenues. Gross profit as a percentage of revenue decreased from 81% in 2004 to 80% in 2005. Gross profit for products decreased to 79% in 2005 compared to 82% in 2004. This decline was driven by increased sales volume on products containing a hardware component, primarily the SafeWord token sales, which have a lower gross profit margin than our software products. Gross margins were also reduced as a result of a larger portion of business being transacted with channel partners versus direct to end users in 2005 as compared to 2004. Gross profit for services was 83% in 2005 compared to 80% in 2004. The improvement in the gross profit rate for services was primarily driven by our services revenue growth outpacing the growth of our services costs in 2005 compared to 2004.

Operating Expenses. Operating expenses consist of selling and marketing, research and development, and general and administrative expenses. Total operating expenses increased 5% to $66.8 million for 2005, up from $63.8 million in 2004. This increase was driven primarily by an inflationary increase in payroll and related costs and inflationary increases in corporate costs. As a percentage of revenue, total operating expenses were 61% for 2005 compared to 68% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of operating expenses during 2005 compared to 2004.

Selling and Marketing. Selling and marketing expenses consist primarily of salaries, commissions, and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, public relations, travel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Selling and marketing expenses increased 3% to $42.3 million in 2005, up from $41.2 million in 2004. This increase was driven primarily by inflationary increases in payroll and related costs, an increase in commission expense due to expanding revenues, and inflationary increases in allocated corporate costs. As a percentage of revenue, selling and marketing expenses were 39% in 2005 compared to 44% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of selling and marketing expenses during 2005 compared to 2004.

Research and Development. Research and development expenses consist primarily of salaries and benefits for our product development personnel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Research and development expenses increased 5% to $16.8 million in 2005, up from $16.1 million in 2004. This increase was driven by inflationary increases in payroll, benefits and allocated corporate costs. As a percentage of revenue, research and development expenses were 15% for the year compared to 17% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of research and development expenses during 2005 compared to 2004.

General and Administrative. General and administrative expenses consist primarily of salaries, benefits and related expenses for our executive, finance and legal personnel, directors and officers insurance and allocations of corporate costs, which include information technology, facilities and human resources expenses. General and administrative expenses increased 11% to $7.2 million in 2005, up from $6.5 million in 2004. This increase was driven primarily by an increase in audit and legal fees, inflationary increases in allocated corporate costs, and to a lesser extent, inflationary increases in payroll and benefits. As a percentage of revenue, general and administrative expenses were 7% in both 2005 and 2004. This rate remained consistent compared to prior year, despite the increase in our general and administrative expenses, due to revenue growth being consistent with the growth of general and administrative expenses in 2005 compared to 2004.

Other Income. Other income was $1.6 million in 2005, an increase from $607,000 in 2004. The increase reflects higher interest rates on higher cash balances in 2005 as compared to 2004.

Income Taxes. We incurred tax expenses of $608,000, consisting of $349,000 for U.S. Federal alternative minimum tax expense, $58,000 for state income tax expense, and $201,000 for various foreign income taxes, in 2005 compared to no tax expense recognized in 2004. Federal alternative minimum tax was provided for in 2005 on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carry forward which we have available. This is in accordance with applicable tax law. The tax position provided for in the income tax provisions prior to 2005 did not include alternative minimum taxable income. Tax expense of $283,000 incurred for various foreign income taxes and $62,000 incurred for state income tax in 2004 was offset by the reversal of a like amount of the previously established valuation allowance against our deferred tax asset. We have assessed the likelihood that our net deferred tax assets will be realized. The computations of our deferred tax assets and valuation allowance are based on taxable income we expect to earn on sales of existing products, and projected interest and other income over the next three years. Realization of the $3.6 million of net deferred tax assets is dependent upon our ability to generate sufficient future taxable income and the implementation of tax planning strategies. We have determined that it is more likely than not that the net deferred tax assets will be realized based on expected levels of future taxable income in the U.S. and certain foreign jurisdictions and the implementation of tax planning strategies. Our expectations regarding future profitability may change due to future market conditions, changes in tax laws and other factors. Future taxable income of $9.4 million is required to realize the $3.6 million deferred tax asset at December 31, 2005. We had total net operating loss carryforwards of approximately $177.7 million at December 31, 2005. Of these carryforwards, $49.9 million relates to stock option exercises and $59.6 million relates to acquired N2H2 net operating losses, which currently have a full valuation allowance, and when realized for financial statement purposes will not result in a reduction in income tax expense. Rather, the benefit from the stock option exercises will be recorded as an increase to additional paid-in capital and the benefit from the N2H2 net operating loss carryforwards will be recorded as a decrease to goodwill. Of the remaining benefit associated with the carryforwards, approximately $58.8 million have yet to be recognized as a benefit in the consolidated statement of operations. However, there are no assurances that these carryforwards will be available to offset future income tax expense when taxable income is realized.

Deferred taxes are required to be measured at the regular tax rate. An analysis recently completed of our regular tax rate, indicated that our tax rate had changed. Accordingly the deferred tax components, including the valuation allowance, were adjusted as a result of applying the appropriate rate. The deferred tax components include the benefit of the alternative tax credit carry forward. See Note 12 of the Notes to the Consolidated Financial Statements regarding the tax effect of these items in 2005.

Estimates were used in the determination of our provision for income taxes, current income taxes payable, as well as in our deferred tax asset and liability analysis. These estimates take into account current tax laws and our interpretation of these current tax laws within the various taxing jurisdictions within which we operate. Changes in the tax laws or our interpretation of tax laws and the resolution of future audits could impact our provision for income taxes.

Liquidity and Capital Resources

At December 31, 2006, our principal source of liquidity was $8.2 million of cash, representing a $41.8 million decrease from December 31, 2005. Our investments decreased $30.7 million from $31.1 million at December 31, 2005 to $457,000 at December 31, 2006. These decreases were primarily due to $95.0 million in cash paid directly by us to CipherTrust shareholders for the CipherTrust acquisition, $18.9 million in cash paid directly by us to CyberGuard shareholders for the CyberGuard acquisition, offset by $36.1 million provided by operating activities and $8.1 million from the exercise of stock options and sale of common stock through our employee stock purchase plan (ESPP). At December 31, 2006, we have future payments of $138.5 million on our debt commitment and net future payments under non-cancelable operating leases of $23.2 million. We expect to generate cash during 2007 as we expect billings to continue to grow at a faster rate than operating expenses.

Last year we financed our operations primarily with cash generated from operations, as well as through sales of our equity securities and borrowings on our credit facility. In 2006, we utilized and paid back $8.5 million on our $20.0 million revolving credit facility.

Net cash provided by operating activities of $36.1 million for the twelve months ended December 31, 2006, was comprised of $41.8 million in net non-cash related expenses, a $43.9 million increase in deferred revenue, and a $8.4 million increase in accounts payable and accrued payroll offset by a $27.4 million net loss, a $12.1 million increase in accounts receivable, a $4.3 million decrease in accrued expenses and a $14.3 million decrease in acquisition reserves. Net cash provided by operations was driven by the increase in our billings outpacing the increase in our operating expenses. Terms for cash collections received from customers and cash payments made to vendors were consistent with normal business practices.

Net cash used in investing activities of $239.3 million for the twelve months ended December 31, 2006, consisted of a $187.7 million cash outlay for the acquisition of CipherTrust, $69.1 million cash outlay for the acquisition of CyberGuard, and $11.8 million for capital additions, net of $31.0 million in cash received from net sales/maturities of investments. The capital additions were used for furnishing our new St. Paul, Minnesota facility, computer equipment and technology upgrades.

Net cash provided by financing activities of $163.0 million for the twelve months ended December 31, 2006 consisted primarily of $84.9 million received from debt financing, net of transaction fees of $3.1 million and a principal repayment of $2.0 million, which was used to finance the CipherTrust acquisition, $69.9 million received from the issuance of preferred stock, net of transaction fees, which was used to finance the CyberGuard acquisition, and $8.1 million related to the exercise of stock options and sale of common stock through our ESPP.

We anticipate using available cash to fund growth in operations, invest in capital equipment, acquire businesses, license technology or products related to our line of business, and make additional payments on our long-term debt. We expect to spend approximately $12.0 million on capital expenditures in 2007.

A summary of our total contractual cash obligations as of December 31, 2006 is as follows (in thousands):

		Payments Due by Period			
	Total	Less Than One Year	One to Three Years	Three to Five Years	After Five Years
Operating leases, net of subleases . .	$ 23,233	$ 5,264	$ 7,419	$ 4,196	$ 6,354
Principal and interest payments on debt	$138,509	$ 7,730	$16,290	$16,877	$ 97,612
Total contractual cash obligations . . .	$161,742	$12,994	$23,709	$21,073	$103,966

We believe that we have sufficient financial resources available to fund our current working capital and capital expenditure requirements for at least the next twelve months. In addition to the cash on hand, we have a $20.0 million revolving credit facility available pursuant to a credit facility agreement with a syndicate of banks led by Citigroup and UBS Investment Bank which was signed in August 2006. We intend to utilize the funds available through the credit facility for general working capital and ongoing corporate purposes as deemed necessary.

Our credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain financial covenants, on a quarterly basis, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We are in compliance with all covenants as of December 31, 2006.

Disclosures about Off-Balance Sheet Arrangements

We did not have any off-balance sheet arrangements as of December 31, 2006 or 2005.

Critical Accounting Policies and Estimates

Our discussion of the financial condition and results of operations are based upon the consolidated financial statements, which have been prepared in conformity with U.S. generally accepted accounting principles. The preparation of our financial statements requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, revenues and expenses, and related disclosure of any contingent assets and liabilities at the date of the financial statements. Management regularly reviews its estimates and assumptions, which are based on historical factors and other factors that are believed to be relevant under the circumstances. Actual results may differ from these estimates under different assumptions, estimates, or conditions.

Critical accounting policies are defined as those that are reflective of significant judgments and uncertainties, and potentially result in materially different results under different assumptions and conditions. See Note 1 of the Notes to Consolidated Financial Statements for additional discussion of the application of these and other accounting policies.

Revenue Recognition. We derive our revenue primarily from two sources: (i) sales of products, including hardware, subscriptions, software licenses, and royalties and (ii) sales of services, including maintenance arrangements to provide upgrades and customer support, professional services, and contracted development work. We recognize revenue in accordance with Statement of Position (SOP) 97-2, "Software Revenue Recognition," as modified by SOP 98-9. Revenue from products is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed and determinable, and collection is probable. Subscription-based contracts are generally for 12, 24 or 36 months in duration. Subscription revenue along with maintenance revenue for providing product upgrades and customer support are deferred and recognized ratably over the service period beginning with the month the subscription or service begins.

When arrangements contain multiple elements and vendor specific objective evidence (VSOE) of fair value exists for all undelivered elements, we recognize revenue for the delivered elements using the residual method. For arrangements containing multiple elements where VSOE of fair value does not exist for all undelivered elements, we defer revenue for the delivered and undelivered elements and then recognize revenue on all elements over the service period. In instances where an entire arrangement is deferred due to lack of VSOE of fair value on an undelivered element, the revenue recognized over the service period is allocated to products and services revenue based on the value of the elements as presented on the customer's purchase order which approximates an allocation proportionate to our list price. We also identify costs (primarily hardware component costs) that are directly associated with product revenues that have been deferred due to lack of VSOE of fair value on an undelivered element and we defer these costs at the time of shipment and recognize them as cost of sales in proportion to the product revenue as it is recognized over the service term.

We sell our products either directly to an end-user, or indirectly through our channel of resellers and distributors (our channel partners). When selling through our channel we require our channel partners to provide evidence of end-user sell-through. If we are unable to obtain end-user evidence at the time we fulfill the order from a channel partner, we do not recognize revenue until the channel partner supplies end-user information, the product has been shipped, and all other criteria of SOP 97-2 have been met, with the exception of sales to our distributors who stock our SnapGear product line. We recognize revenue, net of estimated returns, upon shipment of our SnapGear product line as we have sufficient return history to establish a reserve and we are not able to receive end-user evidence due to the high-volume sales of this low-price point product.

Allowance for Doubtful Accounts. We make estimates regarding the collectibility of our accounts receivables. When we evaluate the adequacy of our allowance for doubtful accounts, we consider multiple factors including historical write-off experience, the need for specific customer reserves, the aging of our receivables, customer creditworthiness, changes in our customer payment cycles, and current economic trends. Historically, our allowance for doubtful accounts has been adequate based on actual results. If the financial condition of our customers were to deteriorate, resulting in an impairment of their ability to make payments, additional allowances may be required.

Business Combinations. When we acquire businesses, we allocate the purchase price to tangible assets and liabilities and identifiable intangible assets acquired. Any residual purchase price is recorded as goodwill. The allocation of the purchase price requires management to make significant estimates in determining the fair values of assets acquired and liabilities assumed, especially with respect to intangible assets. These estimates are based on historical experience and information obtained from the management of the acquired companies. These estimates can include, but are not limited to, the cash flows that an asset is expected to generate in the future, the appropriate weighted average cost of capital, and the cost savings expected to be derived from acquiring an asset. These estimates are inherently uncertain and unpredictable. In addition, unanticipated events and circumstances may occur which may affect the accuracy or validity of such estimates.

We assess the impairment of goodwill annually, or more often if events or changes in circumstances indicate that the carrying value may not be recoverable. We evaluate goodwill for impairment by comparing the fair value of our reporting unit to its carrying value, including the goodwill allocated to that reporting unit. To determine our reporting unit's fair value in the current year evaluation, we used a valuation technique based on multiples of revenue. If management's estimates of future operating results change, or if there are changes to other assumptions, the estimate of the fair value of our goodwill could change significantly. Such change could result in goodwill impairment charges in future periods, which could have a significant impact on our consolidated financial statements.

We assess the impairment of acquired developed technology and other identifiable intangible assets whenever events or changes in circumstances indicate that an asset's carrying amount may not be recoverable. An impairment loss would be recognized when the sum of the estimated future cash flows expected to result from the use of the asset and its eventual disposition is less than its carrying amount. Such impairment loss would be measured as the difference between the carrying amount of the asset and its fair value. Our cash flow assumptions are based on historical and forecasted revenue, operating costs, and other relevant factors. If management's estimates of future operating results change, or if there are changes to other assumptions, the estimate of the fair value of our acquired developed technology and other identifiable intangible assets could change significantly. Such change could result in impairment charges in future periods, which could have a significant impact on our consolidated financial statements.

Deferred Tax Assets. We account for income taxes under SFAS No. 109, "Accounting for Income Taxes," which requires recognition of deferred tax liabilities and assets for the expected future tax consequences of events that have been included in our financial statements or tax returns. Under this method, deferred tax liabilities and assets are determined based on the difference between the financial statement and tax basis of assets and liabilities, using enacted tax rates in effect for the year in which the differences are expected to reverse. SFAS No. 109 requires the consideration of a valuation allowance for deferred tax assets if it is "more likely than not" that some component or all of the benefits of deferred tax assets will not be realized.

Share-Based Compensation. Prior to January 1, 2006, we accounted for share-based employee compensation plans under the measurement and recognition provisions of Accounting Principles Board (APB) Opinion No. 25, "Accounting for Stock Issued to Employees," and related Interpretations, as permitted by SFAS No. 123, "Accounting for Stock-Based Compensation." Accordingly, we recorded no share-based employee compensation expense for options granted under our current stock option plans during the year ended December 31, 2005 as all options granted under those plans had exercise prices equal to the fair market value of our common stock on the date of grant. We also recorded no compensation expense in those periods in connection with our Employee Stock Purchase Plan (ESPP) as the purchase price of the stock was not less than 85% of the lower of the fair market value of our common stock at the beginning of each offering period or at the end of each purchase period. In accordance with SFAS No. 123 and SFAS No. 148, "Accounting for Stock-Based Compensation – Transition and Disclosure," we provided pro forma net income and net income per share disclosures for each period prior to the adoption of SFAS No. 123(R), "Share-Based Payment," as if we had applied the fair value-based method in measuring compensation expense for our share-based compensation plans.

Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R), using the modified prospective transition method. Under that transition method, we recognized compensation expense for share-based payments that vested during the year ended December 31, 2006 using the following valuation methods: (a) for share-based payments granted prior to, but not yet vested as of, January 1, 2006, the grant date fair value was estimated in accordance with the original provisions of SFAS No. 123, and (b) for share-based payments granted on or after January 1, 2006, the grant date fair value was estimated in accordance with the provisions of SFAS No. 123(R). Because we elected to use the modified prospective transition method, results for prior periods have not been restated. In March 2005, the Securities and Exchange Commission issued Staff Accounting Bulletin (SAB) No. 107, "Share-Based Payment," which provides supplemental implementation guidance for SFAS No. 123(R). We have applied the provisions of SAB No. 107 in our adoption of SFAS No. 123(R). We estimate the fair value of stock options granted and the discount offered through our ESPP using the Black Scholes model, which requires the input of highly subjective assumptions. See Note 10 for information on the impact of our adoption of SFAS No. 123(R) and the assumptions we use to calculate the fair value of share-based employee compensation. In addition, we began offering restricted shares in 2006 and we intend to continue to do so in the future.

Derivative Instrument. In September 2006, we entered into an interest rate cap agreement which is required to be accounted for under SFAS No. 133, "Accounting for Derivative Instruments and Hedging Activities." SFAS No. 133 establishes accounting and reporting standards for derivative instruments, including certain derivative instruments embedded in other contracts, and for hedging activities. It requires that an entity recognize all derivatives as either assets or liabilities in the statement of financial position and measure those instruments at fair value. If certain conditions are met, a derivative may be specifically designated as (a) a hedge of the exposure to changes in the fair value of a recognized asset or liability or an unrecognized firm commitment, (b) a hedge of the exposure to variable cash flows of a forecasted transaction, or (c) a hedge of the foreign currency exposure of a net investment in a foreign operation, an unrecognized firm commitment, an available-for-sale security, or a foreign-currency-denominated forecasted transaction. Our interest rate cap agreement applies to (b), referred to as a cash flow hedge. For a derivative that is designated as a cash flow hedge the effective portion of the derivative's gain or loss is initially reported as a component of other comprehensive income and subsequently reclassified into earnings when the forecasted transaction affects earnings. The ineffective portion of the gain or loss is immediately recognized in income.

Inflation

To date, we have not been significantly affected by inflation.

Recently Issued Accounting Standards

In July 2006, the FASB issued Interpretation No. 48 (FIN 48), "Accounting for Uncertainty in Income Taxes, an Interpretation of SFAS No. 109." FIN 48 creates a single model to address accounting for uncertainty in tax positions and clarifies the accounting for income taxes by prescribing the minimum recognition threshold a tax position is required to meet before being recognized in the financial statements. Specifically under FIN 48, the tax benefits from an uncertain tax position may be recognized only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities, based upon the technical merits of the position. FIN 48 also provides guidance on de-recognition, measurement, classification, interest and penalties, accounting in interim periods, disclosure and transition. FIN 48 is effective for fiscal years beginning after December 15, 2006. As prescribed in the interpretation, the cumulative effect of applying the provisions of FIN 48 will be reported as an adjustment to the opening balance of retained earnings at January 1, 2007. We will adopt FIN 48 effective January 1, 2007 as required. We are currently evaluating the potential impact which the adoption of FIN 48 will have on our financial position, cash flows, and results of operations.

In September 2006, the FASB issued SFAS No. 157, "Fair Value Measurements." SFAS No. 157 establishes a framework for measuring fair value in generally accepted accounting principles, clarifies the definition of fair value within that framework, and expands disclosures about the use of fair value measurements. SFAS No. 157 is intended to increase consistency and comparability among fair value estimates used in financial reporting. As such, SFAS No. 157 applies to all other accounting pronouncements that require (or permit) fair value measurements, except for the measurement of share-based payments. SFAS No. 157 does not apply to accounting standards that require (or permit) measurements that are similar to, but not intended to represent, fair value. Fair value, as defined in SFAS No. 157, is the price to sell an asset or transfer a liability and therefore represents an exit price, not an entry price. The exit price is the price in the principal market in which the reporting entity would transact. Further, that price is not adjusted for transaction costs. SFAS No. 157 is effective for fiscal years beginning after November 15, 2007, and interim periods within those fiscal years. SFAS No. 157 will be applied prospectively as of the beginning of the fiscal year in which it is initially applied. We are currently assessing the impact of adoption of SFAS No. 157.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We develop products in the U.S., Australia, and Germany and sell them worldwide. As a result, our financial results could be affected by factors such as changes in foreign currency exchange rates or weak economic conditions in foreign markets. Since our sales are currently priced in U.S. dollars, a strengthening of the dollar could make our products less competitive in foreign markets and our accounts receivable more difficult to collect.

We believe that our international entities are subject to risks typical of any international entity, including, but not limited to: differing economic conditions, changes in political climate, differing tax structures, other regulations and restrictions, and foreign exchange rate volatility. Accordingly, our future results could be materially adversely impacted by changes in these or other factors.

We are exposed to market risk from changes in the interest rates on certain outstanding debt. As of December 31, 2006, we had $88.0 million of outstanding indebtedness. Of this indebtedness, approximately $28.0 million bears interest at rates that fluctuate with changes in certain prevailing interest rates. Based on the average outstanding debt for fiscal 2006, a 100 basis point change in interest rates would change interest expense by approximately $300,000 in fiscal 2007.

We also hold an equity interest in a privately held technology company. This investment was recorded at cost and is reported in other assets on our consolidated balance sheets. As of December 31, 2006 this investment had a carrying value of $2.7 million.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

Our financial statements required by this item are set forth as a separate section of this report. See Part IV, Item 15 of this Form 10-K.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

Not applicable.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

Management of our company is responsible for establishing and maintaining effective disclosure controls and procedures, as defined under Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934. At December 31, 2006, an evaluation was performed, under the supervision and with the participation of management, including our Chief Executive Officer and Chief Financial Officer, of the effectiveness of the design and operation of our disclosure controls and procedures. Based upon that evaluation, the Chief Executive

Officer and Chief Financial Officer concluded that as of December 31, 2006, our disclosure controls and procedures were not effective at the reasonable assurance level, as a result of a material weakness in the internal controls related to accounting for income taxes, to ensure that information required to be disclosed in the Annual Report on Form 10-K was recorded, processed, summarized and reported within the time period required by the Securities and Exchange Commission's rules and forms and accumulated and communicated to management, including our Chief Executive Officer and Chief Financial Officer, to allow timely decisions regarding required disclosure.

Changes in Internal Control Over Financial Reporting

During the quarter ended December 31, 2006, there have been no changes in our internal control over financial reporting that materially affected, or are reasonably likely to materially affect, our internal control over financial reporting, except those relating to the acquisition of CipherTrust, Inc. as of December 31, 2006 and the material weakness indentified below. See Note 2 of the Notes to the Consolidated Financial Statements included in Item 15 for discussion of the acquisition and related financial data. We are in the process of integrating the CipherTrust operations and will be incorporating these operations as part of our internal controls. However, for purposes of this evaluation, the impact of this acquisition on our internal controls over financial reporting has been excluded.

Management's Report on Internal Control Over Financial Reporting

Our management is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rules 13a-15(f) under the Securities Exchange Act of 1934. Our internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with accounting principles generally accepted in the United States. Internal control over financial reporting includes those written policies and procedures that:

- pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of our assets;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America;
- provide reasonable assurance that our receipts and expenditures are being made only in accordance with authorization of our management and directors; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on the consolidated financial statements.

Internal control over financial reporting includes the controls themselves, monitoring and internal auditing practices and actions taken to correct deficiencies as identified.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A material weakness in internal control over financial reporting is a significant deficiency (within the meaning of PCAOB Auditing Standard No. 2), or combination of significant deficiencies, that results in there being more than remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected by employees in the normal course of performing their assigned functions.

Management assessed the effectiveness of our internal control over financial reporting as of December 31, 2006. In making this assessment, management used the criteria set forth by the Committee of Sponsoring

Organizations of the Treadway Commission (COSO) in Internal Control – Integrated Framework. Management's assessment included an evaluation of the design of our internal control over financial reporting and testing of the operational effectiveness of its internal control over financial reporting. Management reviewed the results of its assessment with the Audit Committee of our Board of Directors.

Based on this assessment, management identified, as of December 31, 2006, a material weakness existed in the company's internal control over financial reporting related to the accounting for income taxes. There were ineffective controls relating to the review of our year-end tax provision, including review of the tax technical accounting items where our outside tax consultants typically provide input. This control deficiency resulted in a material misstatement of various income tax balances that was not prevented or detected by management. As a result, material errors in accounting for income taxes occurred, which were corrected prior to the issuance of the annual financial statements. Accordingly management has determined this control deficiency constitutes a material weakness.

Due to the material weakness described above, management concluded that, as of December 31, 2006, the Company's system of internal control over financial reporting related to accounting for income taxes was not effective based on the criteria established in Internal Control—Integrated Framework.

Management's assessment of the effectiveness of internal control over financial reporting as of December 31, 2006 excluded the business operations of CipherTrust, Inc., acquired on August 31, 2006. The acquired business operations excluded represent $66.0 million and $19.1 million of total and net assets, respectively, and $7.1 million of revenues of our related consolidated financial statement amounts as of and for the year ended December 31, 2006.

Our management's assessment of the effectiveness of our internal control over financial reporting as of December 31, 2006 has been audited by Ernst & Young LLP, an independent registered public accounting firm, as stated in their report which is included herein on page 78.

Remediation Plan for Material Weakness in Accounting for Income Taxes

In 2006 we experienced an increased level of complexity in our accounting for income taxes as the result of the CyberGuard and CipherTrust acquisitions which occurred during the year. As a result of this increased complexity we have engaged our outside tax consultants to assist in the review of our tax provision in order for us to have effective review controls over our accounting for income taxes. The review of our tax provision workpapers for the period ended December 31, 2006 was ineffective and the review by our outside tax consultants did not occur, resulting in a material weakness. To remediate the identified material weakness, management plans to ensure that the appropriate levels of review by management and involvement of outside tax consultants will take place in a timely manner in future periods.

PART III

ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT

Incorporated herein by reference is the information under the heading "Election of Directors," "Section 16(a) Beneficial Ownership Reporting Compliance," and "Committees of the Board of Directors," in our Proxy Statement to be filed on or about March 30, 2007. See also Part I, Item 1, "Executive Officers" of this Form 10-K.

We maintain a Code of Business Conduct and Ethics applicable to all our employees. We have also adopted a Code of Ethics for Finance that is applicable to our Chief Executive Officer, Chief Financial Officer, Vice President of Finance, and finance personnel performing functions related to financial reporting. A copy of our Code of Business Conduct and Ethics and our Code of Ethics for Finance, as well as our corporate governance guidelines and the committee charters for each of the committees of the Board of Directors, can be obtained from our Internet website at **www.securecomputing.com** under the Investor Relations page and will be made available free of charge to any shareholder upon request. We intend to disclose any waivers from, or amendments to, the Code of Business Conduct and Ethics and Code of Ethics for Finance by posting a description of such waiver or amendment on our Internet website. However, we have never granted a waiver from either the Code of Business Conduct and Ethics and Code of Ethics for Finance.

ITEM 11. EXECUTIVE COMPENSATION

Incorporated herein by reference is the information appearing in our Proxy Statement which we anticipate filing on or about March 30, 2007, under the headings "Election of Directors," "Compensation Discussion and Analysis (CD&A)," "Compensation Committee Report," "Summary Compensation Table," "2006 Grants of Plan-Based Awards," "2006 Outstanding Equity Awards at Fiscal Year-End," "2006 Option Exercises and Stock Vested," "Director Compensation," and "2006 Potential Payments Upon Termination or Change in Control."

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT

Incorporated herein by reference is the information appearing under the heading "Security Ownership of Principal Stockholders and Management" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

Equity Compensation Plan Information

The following table sets forth information regarding securities authorized for issuance under equity compensation plans:

Plan category	Number of securities to be issued upon exercise of outstanding options, warrants and rights	Weighted-average exercise price of outstanding options, warrants and rights	Number of securities remaining available for future issuance under equity compensation plans
Equity compensation plans approved by stockholders (1)(2)(3)(4)(5)	13,182,418	$9.92	2,367,523
Equity compensation plans not approved by stockholders (6)	3,678,134	4.97	510,197
Total	16,860,552	$8.84	2,877,720

(1) In September 1995, our Board of Directors and stockholders approved our 1995 Omnibus Stock Plan. Under the terms of this Plan, key employees and non-employees may be granted options to purchase up to 11,494,131 shares of our Common Stock. The majority of options granted under this plan have ten year terms and vest either annually over three years, or fully vest at the end of three years. Beginning in 2003, all new stock options granted under this plan vest 25% after the first year and then monthly over the following three years. This plan expired in September 2005.

(2) In connection with our acquisition of N2H2, Inc. in October 2003, we assumed all of the outstanding N2H2 stock options under the 1997 Stock Option Plan, 1999 Stock Option Plan, 1999 Non-Employee Director Plan, 1999/2000 Transition Plan, the 2000 Stock Option Plan, and the Howard Philip Welt Plan (the "N2H2 Plans"), which were converted into options to purchase approximately 420,000 shares of our common stock. All stock options assumed were exercisable and vested. These options were assumed at prices between $1.55 and $258.63 per share, with a weighted average exercise price of $9.45 per share. The options granted under these plans have ten year terms and vest 25% after the first year and then monthly over the following three years.

(3) In connection with our acquisition of CyberGuard in January 2006, we assumed all of the outstanding CyberGuard stock options under the 1994 and 1998 Stock Option Plans which were converted into options to purchase 3,039,545 shares of our common stock. All outstanding stock options assumed were exercisable and vested. These options were assumed at prices between $1.56 and $15.07 per share, with a weighted average exercise price of $7.21 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

(4) In July 2002, our Board of Directors and Compensation Committee approved our 2002 Stock Incentive Plan. In September 2005, our Board of Directors and Compensation Committee approved an amendment and restatement of our 2002 Stock Incentive Plan. Our stockholders approved the amendment and restatement on January 11, 2006. Under the terms of this Plan, key employees and non-employees may be granted options, restricted stock awards, restricted stock units, stock appreciation rights and other similar types of stock awards to purchase up to 6,500,000 shares of our Common Stock. The options granted in 2002 have ten year terms and vest either annually over three years, or fully vest at the end of three years. Beginning in 2003, all options granted under this plan vest 25% after the first year and then monthly over the following three years for employees. Restricted stock awards vest 25% after the first year, then quarterly thereafter over the following three years, unless otherwise approved by the Compensation Committee. All awards granted to non-employee directors vest 100% after the first year.

(5) In connection with our acquisition of CyberGuard in January 2006, we issued a warrant to purchase 1,000,000 shares of our Common Stock pursuant to a securities purchase agreement with Warburg Pincus. The warrant is exercisable at $13.85 per share.

(6) In connection with our acquisition of CipherTrust in August 2006, we assumed all of the outstanding CipherTrust stock options under the 2000 Stock Option Plan which were converted into options to purchase 2,543,662 shares of our common stock. All outstanding stock options assumed were unvested and have seven-year terms. These options were assumed at prices between $0.01 and $6.19 per share, with a weighted average exercise price of $2.88 per share. After the date of acquisition, the options granted under these plans have ten year terms and vest 25% after the first year and then monthly over the following three years.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS

Incorporated herein by reference is the information appearing under the heading "Certain Transactions" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

Incorporated herein by reference is the information appearing under the heading "Relationship with Independent Registered Public Accounting Firm" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

PART IV

ITEM 15. EXHIBITS, FINANCIAL STATEMENT SCHEDULES, AND REPORTS ON FORM 8-K

(a) The following documents are filed as part of this report:

1. Consolidated Financial Statements:

Consolidated Balance Sheets as of December 31, 2006 and 2005
Consolidated Statements of Operations for the years ended December 31, 2006, 2005 and 2004
Consolidated Statements of Stockholders' Equity for the years ended December 31, 2006, 2005 and 2004
Consolidated Statements of Cash Flows for the years ended December 31, 2006, 2005 and 2004
Notes to Consolidated Financial Statements
Report of Independent Registered Public Accounting Firm
Report of Independent Registered Public Accounting Firm – Section 404

2. Consolidated Financial Statement Schedule:

Schedule II – Valuation and Qualifying Accounts. Such schedule should be read in conjunction with the consolidated financial statements. All other supplemental schedules are omitted because of the absence of conditions under which they are required.

(b) Reports on Form 8-K:

On November 14, 2006, we filed an Amendment No. 1 on Form 8-K/A which amends and supplements the Current Report on Form 8-K filed by us on September 7, 2006 pursuant to Item 2.01, "Completion of Acquisition or Disposition of Assets," announcing that on August 31, 2006, we completed the purchase of substantially all of the assets of CipherTrust, Inc. This Amendment No. 1 was filed to include the financial information pursuant to Item 9.01, "Financial Statements and Exhibits."

(c) Exhibits required to be filed by Item 601 of Regulation S-K:

The following exhibits are filed as part of this Annual Report on Form 10-K for the fiscal year ended December 31, 2006:

Exhibit	Description
2.1	Agreement and Plan of Merger, dated as of July 28, 2003, among Secure Computing Corporation, Nitro Acquisition Corp., and N2H2, Inc. is incorporated by reference to the corresponding exhibit to our Registration Statement of Form S-4 (Registration Number 333-107804) filed with the SEC on August 8, 2003.
2.2	Agreement and Plan of Merger, dated as of August 17, 2005, by and among Secure Computing Corporation, Bailey Acquisition Corp., and CyberGuard Corporation is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
2.3	Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on July 13, 2006.
2.4	First Amendment, dated July 14, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on July 18, 2006.

Exhibit	Description
2.5	Second Amendment, dated August 1, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on August 7, 2006.
2.6	Third Amendment, dated August 30, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 99.3 to our Current Report on Form 8-K filed with the SEC on September 28, 2006.
3.1	Restated Certificate of Incorporation, effective March 6, 1996, as amended by the Certificate of Amendment of Certificate of Incorporation effective December 11, 1988, the Certificate of Designations of Series E 4% Cumulative Preferred Stock effective January 26, 2000; and the Certificate of Designations of Series F 4% Cumulative Convertible Preferred Stock effective June 30, 2000 is incorporated by reference to the corresponding exhibit to our Amended Quarterly Report on Form 10-Q for the period ended June 30, 2000.
3.2	By-Laws of the Registrant are incorporated by reference to Exhibit 3.3 to our Registration Statement on Form S-1 (Registration Number 33-97838).
3.3	Certificate of Designations, Preferences and Rights of Series A Convertible Preferred Stock is incorporated by reference to Exhibit 3.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
4.1	Specimen of common stock certificate is incorporated by reference to the corresponding exhibit to Amendment No. 2 to our Registration Statement on Form S-1 (Registration Number 33-97838).
4.2	Amended and Restated 1995 Omnibus Stock Plan is incorporated by reference to the Exhibit 10.1 to our Current Report on Form 8-K filed on October 8, 1999.
4.3	2002 Stock Incentive Plan is incorporated by reference to Exhibit 99.1 to our Registration Statement on Form S-8 (Registration Number 333-115583) filed with the SEC on January 19, 2006.
4.4	CyberGuard Corporation Stock Incentive Plan is incorporated by reference to Exhibit 4.1 to CyberGuard Corporation's Registration Statement on Form S-8 (Registration Number 33-88448) filed with the SEC on January 13, 1995.
4.5	CyberGuard Corporation Third Amended and Restated Employee Stock Option Plan is incorporated by reference to CyberGuard Corporation's Proxy Statement filed on December 13, 2003.
4.6	Warrant by and among Secure Computing Corporation and Warburg Pincus IX, L.P. is incorporated by reference to Exhibit 4.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
4.7	CipherTrust, Inc. 2000 Stock Option Plan.
10.1	Employment Agreement with John McNulty is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended March 31, 1999.
10.2	Employment Agreement with Timothy Steinkopf is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended June 30, 2001.
10.3	Employment Agreement with Vince Schiavo is incorporated by reference to Exhibit 10.1 of our Quarterly Report of Form 10-Q for the period ended June 30, 2001.
10.4	Employment Agreement with Michael Gallagher is incorporated by reference to the corresponding exhibit of our Annual Report of Form 10-K for the period ended December 31, 2004.
10.5	Employment Agreement with Mary Budge is incorporated by reference to the corresponding exhibit of our Annual Report of Form 10-K for the period ended December 31, 2004.

Exhibit	Description
10.6	Securities Purchase Agreement, dated as of August 17, 2005, by and among Secure Computing Corporation and Warburg Pincus IX, L.P. is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
10.7	Amendment No. 1 to the Securities Purchase Agreement by and among Secure Computing Corporation and Warburg Pincus IX, L.P. dated December 9, 2005 is incorporated by reference to Exhibit 99.1 to our Current Report on Form 8-K filed with the SEC on December 13, 2005.
10.8	Form of Indemnification Agreement between the Company, and Cary Davis dated January 31, 2006; Robert J. Frankenberg dated January 31, 2006; James Jordan dated February 1, 2006; John McNulty dated February 1, 2006; Stephen Puricelli dated January 31, 2006; Eric Rundquist dated January 31, 2006; Richard Scott dated January 31, 2006; and Alexander Zakupowsky, Jr. dated February 1, 2006 is incorporated by reference to Exhibit 10.6 to our Current Report on Form 8-K filed with the SEC on January 31, 2006.
10.9	Employment Agreement with Jay Chaudhry is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.10	Employment Agreement with Atri Chatterjee is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.11	Employment Agreement with Paul Judge is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.12	Senior Secured Credit Facilities Commitment Letter, dated as of July 11, 2006, from Citigroup, is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on July 13, 2006.
10.13	Amended and Restated Senior Secured Credit Facilities Commitment Letter, dated as of July 14, 2006, from Citigroup, is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on July 18, 2006.
10.14	Form of Restricted Stock Award Agreement—Secure Computing Corporation 2002 Stock Incentive Plan.
23.1	Consent of Ernst & Young LLP.
24.1	Power of Attorney (See page 81)
31.1	Certification of Chief Executive Officer Pursuant to Section 302 of Sarbanes-Oxley Act of 2002.
31.2	Certification of Chief Financial Officer Pursuant to Section 302 of Sarbanes-Oxley Act of 2002.
32.1	Certification by Chairman, President and Chief Executive Officer Pursuant to Section 906 of Sarbanes-Oxley Act of 2002.
32.2	Certification by Senior Vice President and Chief Financial Officer Pursuant to Section 906 of Sarbanes-Oxley Act of 2002.

SECURE COMPUTING CORPORATION
CONSOLIDATED BALANCE SHEETS
(in thousands, except share and per share amounts)

	December 31, 2006	December 31, 2005
ASSETS		
Current assets		
Cash and cash equivalents	$ 8,249	$ 50,039
Investments and restricted cash	457	31,140
Accounts receivable (net of reserves of 2006 - $1,427; 2005 - $272)	63,636	29,795
Inventory (net of reserves of 2006 - $472; 2005 - $264)	4,078	2,174
Deferred income taxes	—	3,604
Other current assets	13,948	4,869
Total current assets	90,368	121,621
Property and equipment		
Computer equipment and software	22,605	12,490
Furniture and fixtures	2,897	326
Leasehold improvements	2,795	1,093
	28,297	13,909
Accumulated depreciation	(13,997)	(10,068)
	14,300	3,841
Goodwill	533,659	39,230
Intangible assets (net of accumulated amortization of 2006 - $18,782; 2005 -$1,974)	78,388	1,814
Other assets	7,413	5,257
Total assets	$ 724,128	$171,763
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities		
Accounts payable	$ 12,442	$ 2,997
Accrued payroll	12,035	4,690
Accrued expenses	6,365	2,377
Acquisition reserves	1,418	389
Deferred revenue	86,612	29,097
Total current liabilities	118,872	39,550
Acquisition reserves, net of current portion	1,591	364
Deferred revenue, net of current portion	35,671	9,966
Deferred tax liability	7,672	—
Debt, net of fees	85,023	—
Total liabilities	248,829	49,880
Convertible preferred stock, par value $.01 per share: Authorized – 2,000,000 shares; issued and outstanding shares – December 31, 2006 – 700,000 and 2005 – none	65,558	—
Stockholders' equity		
Common stock, par value $.01 per share: Authorized – 100,000,000 shares; issued and outstanding shares – December 31, 2006 – 65,008,509 and December 31, 2005 – 37,021,089	651	370
Additional paid-in capital	538,616	205,970
Accumulated deficit	(127,249)	(83,698)
Accumulated other comprehensive loss	(2,277)	(759)
Total stockholders' equity	409,741	121,883
Total liabilities and stockholders' equity	$ 724,128	$171,763

See accompanying notes.

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except share and per share amounts)

	Year Ended December 31,		
	2006	2005	2004
Revenue			
Products	$115,628	$ 79,339	$67,625
Services	61,069	29,836	25,753
Total revenues	176,697	109,175	93,378
Cost of revenues			
Products	31,540	16,876	12,335
Services	11,756	5,173	5,052
Amortization of purchased intangibles	5,862	—	—
Total cost of revenues	49,158	22,049	17,387
Gross profit	127,539	87,126	75,991
Operating expenses			
Selling and marketing	84,505	42,309	41,201
Research and development	34,073	16,781	16,106
General and administrative	13,608	7,189	6,456
Amortization of purchased intangibles	10,626	496	—
Litigation settlement	2,500	—	—
	145,312	66,775	63,763
Operating (loss)/income	(17,773)	20,351	12,228
Other (expense)/income	(120)	1,631	607
(Loss)/income before taxes	(17,893)	21,982	12,835
Income tax expense	(9,505)	(608)	—
Net (loss)/income	$ (27,398)	$ 21,374	$12,835
Preferred stock accretion	(3,550)	—	—
Charge from beneficial conversion of preferred stock	(12,603)	—	—
Net (loss)/income applicable to common shareholders	$ (43,551)	$ 21,374	$12,835
Basic (loss)/earnings per share	$ (0.76)	$ 0.59	$ 0.36
Weighted average shares outstanding - basic	57,010	36,338	35,576
Diluted (loss)/earnings per share	$ (0.76)	$ 0.57	$ 0.34
Weighted average shares outstanding - diluted	57,010	37,709	37,256

See accompanying notes.

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY
(in thousands, except share amounts)

	Preferred Stock		Common Stock		Additional Paid-In Capital	Accumulated Deficit	Accumulated Other Comprehensive Loss	Total Stockholders' Equity
	Shares	Par Value	Shares	Par Value				
BALANCE, December 31, 2003 ...	—	—	34,953,772	350	190,090	(117,907)	(519)	72,014
Comprehensive income:								
Net income for the year	—	—	—	—	—	12,835	—	12,835
Foreign currency translation adjustment	—	—	—	—	—		(183)	(183)
Unrealized loss on investments	—	—	—	—	—	—	(2)	(2)
Total comprehensive income								12,650
Exercise of employee stock options	—	—	678,451	6	5,787	—	—	5,793
Employee stock purchase plan activity	—	—	165,472	2	1,367	—	—	1,369
BALANCE, December 31, 2004 ...	—	—	35,797,695	358	197,244	(105,072)	(704)	91,826
Comprehensive income:								
Net income for the year	—	—	—	—	—	21,374	—	21,374
Foreign currency translation adjustment	—	—	—	—	—	—	(61)	(61)
Unrealized gain on investments	—	—	—	—	—	—	6	6
Total comprehensive income								21,319
Exercise of employee stock options	—	—	1,059,050	10	7,364	—	—	7,374
Employee stock purchase plan activity	—	—	164,344	2	1,362	—	—	1,364
BALANCE, December 31, 2005 ...	—	$—	37,021,089	$370	$205,970	$ (83,698)	$ (759)	$121,883
Comprehensive loss:								
Net loss for the year	—	—	—	—	—	(27,398)	—	(27,398)
Foreign currency translation adjustment	—	—	—	—	—	—	(1,539)	(1,539)
Unrealized gain on investments	—	—	—	—	—	—	2	2
Unrealized gain on interest rate cap	—	—	—	—	—	—	19	19
Total comprehensive loss								(28,916)
Exercise of employee stock options	—	—	1,418,544	15	6,380	—	—	6,395
Employee stock purchase plan activity	—	—	278,706	3	1,746	—	—	1,749
Share-based compensation expense	—	—	—	—	10,556	—	—	10,556
Issuance of shares for CyberGuard acquisition	—	—	16,290,170	163	188,313	—	—	188,476
Fair value of CyberGuard options assumed in acquisition	—	—	—	—	29,326	—	—	29,326
Beneficial conversion charge for preferred stock	—	—	—	—	12,603	(12,603)	—	—
Preferred stock accretion	—	—	—	—	—	(3,550)	—	(3,550)
Issuance of warrants, net of fees	—	—	—	—	7,937	—	—	7,937
Issuance of shares for CipherTrust acquisition	—	—	10,000,000	100	68,000	—	—	68,100
Fair value of CipherTrust options assumed in acquisition	—	—	—	—	7,785	—	—	7,785
BALANCE, December 31, 2006 ...	—	$—	65,008,509	$651	$538,616	$(127,249)	$(2,277)	$409,741

See accompanying notes.

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

	Year Ended December 31,		
	2006	**2005**	**2004**
Operating activities			
Net (loss)/income	$ (27,398)	$ 21,374	$ 12,835
Adjustments to reconcile net (loss)/income to net cash provided by operating activities:			
Depreciation	4,554	2,214	2,515
Amortization of intangible assets	17,011	881	887
Loss on disposals of property and equipment and intangible assets	999	486	48
Amortization of debt fees	155	—	—
Deferred income taxes	8,486	—	(345)
Share-based compensation	10,556	—	—
Changes in operating assets and liabilities, net of acquisitions:			
Accounts receivable	(12,112)	(9,532)	(2,795)
Inventory	161	621	(1,566)
Other current assets	(38)	619	(970)
Accounts payable	5,299	419	(133)
Accrued payroll	3,076	630	551
Accrued expenses	(4,263)	845	1,191
Acquisition reserves	(14,296)	(619)	(2,224)
Deferred revenue	43,933	9,616	4,006
Net cash provided by operating activities	36,123	27,554	14,000
Investing activities			
Proceeds from sales/maturities of investments	46,434	13,193	17,528
Purchases of investments	(15,406)	(29,921)	(10,355)
Purchase of property and equipment, net	(11,841)	(2,496)	(1,553)
Increase in intangibles and other assets	(1,785)	(4,867)	(802)
Cash paid for business acquisitions, net of cash acquired	(256,743)	—	—
Net cash (used in)/provided by investing activities	(239,341)	(24,091)	4,818
Financing activities			
Proceeds from revolving debt	8,500	—	—
Proceeds from term debt, net of fees	86,868	—	—
Proceeds from issuance of preferred stock and warrant, net of fees	69,945	—	—
Proceeds from issuance of common stock	8,144	8,738	7,162
Repayments of term and revolving debt	(10,500)	—	—
Net cash provided by investing activities	162,957	8,738	7,162
Effect of exchange rates	(1,529)	(61)	(182)
Net (decrease)/increase in cash and cash equivalents	(41,790)	12,140	25,798
Cash and cash equivalents, beginning of year	50,039	37,899	12,101
Cash and cash equivalents, end of year	$ 8,249	$ 50,039	$ 37,899
Supplemental Cash Flow Disclosures:			
Common stock issued for purchase of CyberGuard Corporation.	$ 188,476	—	—
Common stock issued for purchase of CipherTrust, Inc	$ 68,100	—	—
Interest paid	$ 2,711	—	—

See accompanying notes.

SECURE COMPUTING CORPORATION
NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

1. Summary of Significant Accounting Policies

Organization

Secure Computing Corporation is a global leader in enterprise gateway security. Founded in 1989, we have been securing the connections between people and information for nearly 20 years. We use our broad expertise in security technology to develop enterprise gateway security solutions that allow organizations to exchange critical information safely with their customers, partners and employees using trusted connections. Specializing in delivering enterprise-class solutions that secure Web, email, and network connectivity, we are proud to be the global security solutions provider to some of the most mission-critical network environments in the world.

Basis of Consolidation

The consolidated financial statements include the accounts of Secure Computing and our wholly-owned subsidiaries. All intercompany balances and transactions have been eliminated in consolidation.

Use of Estimates

The preparation of financial statements in conformity with U.S. generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the financial statements and accompanying notes. Actual results could differ from those estimates.

Revenue Recognition

We derive our revenue primarily from two sources: (i) sales of products, including hardware, subscriptions, software licenses, and royalties and (ii) sales of services, including maintenance arrangements to provide upgrades and customer support, professional services, and contracted development work. We recognize revenue in accordance with Statement of Position (SOP) 97-2, "Software Revenue Recognition," as modified by SOP 98-9. Revenue from products is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed and determinable, and collection is probable. Subscription-based contracts are generally for 12, 24 or 36 months in duration. Subscription revenue along with maintenance revenue for providing product upgrades and customer support are deferred and recognized ratably over the service period beginning with the month the subscription or service begins.

When arrangements contain multiple elements and vendor specific objective evidence (VSOE) of fair value exists for all undelivered elements, we recognize revenue for the delivered elements using the residual method. For arrangements containing multiple elements where VSOE of fair value does not exist for all undelivered elements, we defer revenue for the delivered and undelivered elements and then recognize revenue on all elements over the service period. In instances where an entire arrangement is deferred due to lack of VSOE of fair value on an undelivered element, the revenue recognized over the service period is allocated to products and services revenue based on the value of the elements as presented on the customer's purchase order which approximates an allocation proportionate to our list price. We also identify costs (primarily hardware component costs) that are directly associated with product revenues that have been deferred due to lack of VSOE of fair value on an undelivered element and we defer these costs at the time of shipment and recognize them as cost of sales in proportion to the product revenue as it is recognized over the service term.

We sell our products either directly to an end-user, or indirectly through our channel of resellers and distributors (our channel partners). When selling through our channel we require our channel partners to provide evidence of end-user sell-through. If we are unable to obtain end-user evidence at the time we fulfill the order from a channel partner, we do not recognize revenue until the channel partner supplies end-user information, the product has been shipped, and all other criteria of SOP 97-2 have been met, with the exception of sales to our distributors who stock our SnapGear product line. We recognize revenue, net of estimated returns, upon shipment of our SnapGear product line as we have sufficient return history to establish a reserve and we are not able to receive end-user evidence due to the high-volume sales of this low-price point product.

Cash Equivalents and Short-Term Investments

We account for investments with the provisions of Statement of Financial Accounting Standards (SFAS) No. 115, "Accounting for Certain Investments in Debt and Equity Securities." SFAS No. 115 addresses the accounting and reporting for investments in fixed maturity securities and for equity securities with readily determinable fair values. Our short-term investments do not include strategic investments. All of our short-term investments are classified as available-for-sale and consist of securities with original maturities in excess of 90 days. We consider investments in instruments purchased with an original maturity of 90 days or less to be cash equivalents. Cash equivalents are carried at cost, which approximates fair value. Short-term investments are carried at fair value as determined by quoted market prices, with unrealized gains and losses, net of tax, reported as a separate component of stockholders' equity. The cost basis of investments that are sold or matured is determined using the specific identification method. Interest and dividends on investments classified as available-for-sale, amortization of premiums and discounts on investments and realized gains and losses and declines in fair value judged to be other-than-temporary on available-for-sale securities are included in other (expense)/income on the consolidated statements of operations. The gross realized gains and losses for the sale or maturity of available-for-sale investments are not material in all periods presented.

Derivative Instrument

In September 2006, we entered into an interest rate cap agreement which is required to be accounted for under SFAS No. 133, "Accounting for Derivative Instruments and Hedging Activities." SFAS No. 133 establishes accounting and reporting standards for derivative instruments, including certain derivative instruments embedded in other contracts, and for hedging activities. It requires that an entity recognize all derivatives as either assets or liabilities in the statement of financial position and measure those instruments at fair value. If certain conditions are met, a derivative may be specifically designated as (a) a hedge of the exposure to changes in the fair value of a recognized asset or liability or an unrecognized firm commitment, (b) a hedge of the exposure to variable cash flows of a forecasted transaction, or (c) a hedge of the foreign currency exposure of a net investment in a foreign operation, an unrecognized firm commitment, an available-for-sale security, or a foreign-currency-denominated forecasted transaction. The interest rate cap agreement applies to (b), referred to as a cash flow hedge. For a derivative that is designated as a cash flow hedge the effective portion of the derivative's gain or loss is initially reported as a component of other comprehensive income or loss (see "Comprehensive (Loss)/Income" below) and subsequently reclassified into earnings when the forecasted transaction affects earnings. The ineffective portion of the gain or loss is immediately recognized in income.

Accounts Receivable

Accounts receivable are initially recorded at fair value upon the sale of products or services to our customers. We make estimates regarding the collectibility of our accounts receivables which we use to record a provision for doubtful accounts. When we evaluate the adequacy of our allowance for doubtful accounts, we consider multiple factors including historical write-off experience, the need for specific customer reserves, the aging of our receivables, customer creditworthiness, changes in our customer payment cycles, and current economic trends. The provision for doubtful accounts is included in selling and marketing expense on the consolidated statement of operations. If the financial condition of our customers were to deteriorate, resulting in an impairment of their ability to make payments, additional allowances may be required.

Equity Investments

We have an equity investment in a privately held company for business and strategic purposes. This investment is included in other assets on our consolidated balance sheets and is accounted for under the cost method as we do not have significant influence over the investee. Under the cost method, the investment is recorded at its initial cost and is periodically reviewed for impairment. Each quarter we assess our compliance with accounting guidance, including the provisions of Financial Accounting Standards Board Interpretation No. (FIN) 46R, "Consolidation of Variable Interest Entities—An Interpretation of ARB No. 51", and any impairment issues. Under FIN 46R, we must consolidate a variable interest entity if we have a variable interest (or combination of variable interests) in the entity that will absorb a majority of the entity's expected losses, receive a majority of the entity's expected residual returns, or both. Currently, our equity investment is not subject to consolidation under FIN 46R as we do not have significant influence over this investee and we do not receive a majority of the returns. During our review for impairment, we examine the investees' actual and forecasted operating results, financial position, and liquidity, as well as business/industry factors in assessing whether a decline in value of an equity investment has occurred that is other-than-temporary. When such a decline in value is identified, the fair value of the equity investment is estimated based on the preceding factors and an impairment loss is recognized in interest and other (expense)/income, in the consolidated statements of operations. During the years ended December 31, 2006 and 2005, we did not recognize an impairment loss on our equity investment.

Inventories

Inventories consist mainly of purchased components and prepaid licenses and are valued at the lower of cost or market using the first-in, first-out (FIFO) method.

Property and Equipment

Property and equipment are carried at cost. Depreciation is calculated using the straight-line method. Estimated useful lives are 3 years for computer equipment and software and 7 years for furniture and fixtures. Leasehold improvements are depreciated over the lesser of the useful life of the asset or the term of the lease.

Financial Instruments

Carrying amounts of financial instruments held by us, which include cash equivalents, short-term investments, restricted cash, accounts receivable, accounts payable and accrued expenses, approximate fair value due to their short-term nature. In the case of our long-term debt, the carrying value of the debt approximates its fair value due to the fact that it is variable-rate debt that reprices frequently. In addition, our credit standing has not changed significantly.

Other Current Assets and Other Assets

Other current assets are carried at cost and consist of unbilled receivables, interest receivable, a derivative instrument, deferred cost of goods sold and prepaid expenses for items such as directors and officers liability insurance, trade shows, royalties, inventory components and foreign taxes to be either expensed or collected within 12 months. Other assets are carried at cost and include a strategic equity investment (see Note 16), rent deposits, and deferred cost of goods sold to be collected or expensed after 12 months.

Income Taxes

We account for income taxes under SFAS No. 109, "Accounting for Income Taxes," which requires recognition of deferred tax liabilities and assets for the expected future tax consequences of events that have been included in our financial statements or tax returns. Under this method, deferred tax liabilities and assets are determined based on the difference between the financial statement and tax basis of assets and liabilities, using enacted tax rates in effect for the year in which the differences are expected to reverse. SFAS No. 109 requires the consideration of a valuation allowance for deferred tax assets if it is "more likely than not" that some component or all of the benefits of deferred tax assets will not be realized.

Goodwill and Other Intangible Assets

Intangible assets consist of patents, trademarks, capitalized software costs, purchased customer and control lists, purchased tradenames, capitalized developed technology and goodwill, all of which are recorded at cost or fair value. Patents, trademarks, tradenames, control lists, and capitalized developed technology are amortized using the straight-line method over the estimated useful lives of the assets, which range up to 17 years. Customer lists are amortized on an accelerated basis based on an attrition rate driven by the estimated revenue stream from acquired customers over a five year period. See accounting policy of capitalized software costs below under Research and Development.

Goodwill is not amortized, but is tested for impairment at the reporting unit level at least annually. If impairment is indicated, a write-down is recorded as an impairment loss in income from operations. An impairment charge is recognized only when the calculated fair value of a reporting unit, including goodwill, is less than its carrying amount. In accordance with SFAS No. 142, "Goodwill and Other Intangible Assets," we completed the required annual impairment tests of goodwill during the fourth quarter of 2006 and 2005 and determined the fair value to be in excess of the carrying value of these assets. Therefore, goodwill was not impaired and no impairment charge was reported.

Long-Lived Assets

We review our long-lived assets and identified finite-lived intangible assets for impairment whenever events or changes in circumstances indicate that the carrying amount of an asset may not be recoverable, except for goodwill as noted above. Recoverability of assets to be held and used is measured by a comparison of the carrying amount of an asset to undiscounted future net cash flows expected to be generated by the assets. If such assets are considered to be impaired, the impairment to be recognized is measured by the amount by which the carrying amount of the assets exceeds the fair value of the assets. There were no such impairments during the periods presented.

Accrued Expenses

At December 31, 2006 and 2005, accrued expenses consisted of costs related to professional fees, royalties, foreign taxes and accrued marketing development funds.

Leases and Deferred Rent

We lease all of our office space. Leases are accounted for under the provisions of SFAS No. 13, "Accounting for Leases," as amended, which requires that leases be evaluated and classified as operating or capital leases for financial reporting purposes. As of December 31, 2006, all of our leases were accounted for as operating leases. For leases that contain rent escalations, we record the total rent payable during the lease term, as determined above, on a straight-line basis over the term of the lease and record the difference between the rents paid and the straight-line rent as a deferred rent.

Concentrations of Credit Risk

Financial instruments that potentially subject us to concentrations of credit risk consist primarily of accounts receivable. We perform ongoing credit evaluations of our customers, generally require customers to prepay for maintenance and maintain reserves for potential losses. Our customer base is primarily composed of businesses throughout the U.S., Europe, Japan, China, the Pacific Rim, and Latin America.

Interest Rate Risk

We have market risk exposure to changing interest rates primarily as a result of our borrowing activities. Our objective in managing our exposure to changes in interest rates is to reduce fluctuations in earnings and cash flows. To achieve these objectives, we use derivative instruments, such as our interest rate cap agreement, to manage risk exposures when appropriate, based on market conditions. We do not enter into derivative agreements for trading or other speculative purposes, nor are we a party to any leveraged derivative instrument.

Foreign Currency Translation and Transactions

Foreign assets and liabilities were translated using the exchange rates in effect at the balance sheet date. Results of operations were translated using average exchange rates throughout the year. Translation gains or losses have been reported in other comprehensive (loss)/income as a component of stockholders' equity. Cumulative foreign currency translation loss balances were $2.3 million and $757,000 at December 31, 2006 and 2005, respectively. Any gains or losses resulting from foreign currency transactions are included in the consolidated statements of operations and are not significant during the periods presented.

Comprehensive (Loss)/Income

The components of our comprehensive (loss)/income are net (loss)/income, foreign currency translation adjustments, unrealized gain on investments and unrealized gain on our interest rate hedge. Comprehensive (loss)/income for all periods presented is included in our consolidated statements of stockholders' equity.

Selling and Marketing

Selling and marketing expenses consist primarily of salaries, commissions, share-based compensation and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, and public relations. Our customer support function, which provides support, training and installation services, is also responsible for supporting our sales representatives and sales engineers throughout the sales cycle by providing them and our prospective customers with technical assistance and, as such, a portion of these costs are included as selling and marketing expense.

Research and Development

Research and development expenditures are charged to operations as incurred. SFAS No. 86, "Accounting for the Costs of Computer Software to Be Sold, Leased, or Otherwise Marketed," requires capitalization of certain software development costs subsequent to the establishment of technological feasibility. Based on our product development process, technological feasibility is established upon completion of a working model. Costs that we incur between completion of the working model and the point at which the product is generally available for sale are capitalized and amortized over their estimated useful life of three years.

Share-Based Compensation

Prior to January 1, 2006, we accounted for share-based employee compensation plans under the measurement and recognition provisions of Accounting Principles Board (APB) Opinion No. 25, "Accounting for Stock Issued to Employees," and related Interpretations, as permitted by SFAS No. 123, "Accounting for Stock-Based Compensation." Accordingly, we recorded no share-based employee compensation expense for options granted under our current stock option plans during the year ended December 31, 2005 as all options granted under those plans had exercise prices equal to the fair market value of our common stock on the date of grant. We also recorded no compensation expense in those periods in connection with our Employee Stock Purchase Plan (ESPP) as the purchase price of the stock was not less than 85% of the lower of the fair market value of our common stock at the beginning of each offering period or at the end of each purchase period. In accordance with SFAS No. 123 and SFAS No. 148, "Accounting for Stock-Based Compensation – Transition and Disclosure," we provided pro forma net income or loss and net income or loss per share disclosures for each period prior to the adoption of SFAS No. 123(R), "Share-Based Payment," as if we had applied the fair value-based method in measuring compensation expense for our share-based compensation plans.

Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R), using the modified prospective transition method. Under that transition method, we recognized compensation expense for share-based payments that vested during 2006 using the following valuation methods: (a) for share-based payments granted prior to, but not yet vested as of, January 1, 2006, the grant date fair value was estimated in accordance with the original provisions of SFAS No. 123, and (b) for share-based payments granted on or after January 1, 2006, the grant date fair value was estimated in accordance with the provisions of SFAS No. 123(R). Because we elected to use the modified prospective transition method, results for prior periods have not been restated. In March 2005, the Securities and Exchange Commission issued Staff Accounting Bulletin (SAB) No. 107, "Share-Based Payment," which provides supplemental implementation guidance for SFAS No. 123(R). We have applied the provisions of SAB No. 107 in our adoption of SFAS No. 123(R). See Note 10 for information on the impact of our adoption of SFAS No. 123(R) and the assumptions we use to calculate the fair value of share-based compensation.

Net (Loss)/Income Per Share

In accordance with SFAS No. 128, "Earnings Per Share," basic net (loss)/income per share is computed by dividing net (loss)/income applicable to common shareholders by the weighted average number of common shares outstanding during the period. Diluted net loss per share is computed by dividing net loss applicable to common shareholders by the weighted average number of common shares outstanding during the period. Diluted net income per share is computed by dividing net income by the combination of dilutive common share equivalents, which consist of stock options and the weighted average number of common shares outstanding.

Recently Issued Accounting Standards

In July 2006, the FASB issued Interpretation No. 48 (FIN 48), "Accounting for Uncertainty in Income Taxes, an Interpretation of SFAS No. 109." FIN 48 creates a single model to address accounting for uncertainty in tax positions and clarifies the accounting for income taxes by prescribing the minimum recognition threshold a tax position is required to meet before being recognized in the financial statements. Specifically under FIN 48, the tax benefits from an uncertain tax position may be recognized only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities, based upon the technical merits of the position. FIN 48 also provides guidance on de-recognition, measurement, classification, interest and penalties, accounting in interim periods, disclosure and transition. FIN 48 is effective for fiscal years beginning after December 15, 2006. As prescribed in the interpretation, the cumulative effect of applying the provisions of FIN 48 will be reported as an adjustment to the opening balance of retained earnings at January 1, 2007. We will adopt FIN 48 effective January 1, 2007 as required. We are currently evaluating the potential impact which the adoption of FIN 48 will have on our financial position, cash flows, and results of operations.

In September 2006, the FASB issued SFAS No. 157, "Fair Value Measurements." SFAS No. 157 establishes a framework for measuring fair value in generally accepted accounting principles, clarifies the definition of fair value within that framework, and expands disclosures about the use of fair value measurements. SFAS No. 157 is intended to increase consistency and comparability among fair value estimates used in financial reporting. As such, SFAS No. 157 applies to all other accounting pronouncements that require (or permit) fair value measurements, except for the measurement of share-based payments. SFAS No. 157 does not apply to accounting standards that require (or permit) measurements that are similar to, but not intended to represent, fair value. Fair value, as defined in SFAS No. 157, is the price to sell an asset or transfer a liability and therefore represents an exit price, not an entry price. The exit price is the price in the principal market in which the reporting entity would transact. Further, that price is not adjusted for transaction costs. SFAS No. 157 is effective for fiscal years beginning after November 15, 2007, and interim periods within those fiscal years. SFAS No. 157 will be applied prospectively as of the beginning of the fiscal year in which it is initially applied. We are currently assessing the impact of adoption of SFAS No. 157.

2. Acquisition of CipherTrust

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. CipherTrust's products provide innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. CipherTrust's products include IronMail, powered by TrustedSource, IronIM, IronMail Edge, IronNet, and RADAR. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and Messaging Gateway Security needs.

The aggregate purchase price was $270.1 million consisting primarily of $188.1 million in cash, the issuance of 10.0 million shares of common stock valued at $68.1 million, the conversion of outstanding CipherTrust stock options into options to purchase 2.5 million shares of our common stock with a fair value of $7.8 million, and direct costs of the acquisition of $6.1 million. The value of the common shares issued was determined based on the average market price of our common shares over the period including two days before and two days after the date that the terms of the acquisition were agreed to and announced. We financed $90.0 million of the CipherTrust acquisition through debt financing obtained from a syndicate of banks led by Citigroup and UBS Investment Bank. See Note 6 for details on the debt financing. As part of the terms of the acquisition, we may issue a $10.0 million note to former CipherTrust shareholders that is subject to the attainment of certain performance conditions to be met by September 30, 2007. Any contingent consideration earned will be recorded as additional goodwill.

The acquisition was accounted for under the purchase method of accounting, and accordingly, the assets and liabilities acquired were recorded at their estimated fair values at the effective date of the acquisition and the results of operations have been included in the consolidated statements of operations since the acquisition date. In accordance with SFAS No. 142, "Goodwill and Other Intangible Assets," goodwill and indefinite lived trademarks recorded as a result of the acquisition will be subject to an annual impairment test and will not be amortized.

The following table summarizes the estimated preliminary fair values of the assets acquired and liabilities assumed at the date of acquisition (in thousands):

		As of August 31, 2006
Cash paid, net of cash acquired		$(187,647)
Current assets		11,399
Property and equipment		1,474
Other long-term assets and indefinite lived assets		8,153
Goodwill		233,857
Intangible assets subject to amortization:		
Intangibles – Customer relationships (60 month useful life)	14,298	
Intangibles – Developed technology (48 month useful life)	21,445	
		35,743
Total assets acquired		102,979
Current liabilities		6,853
Acquisition reserve		7,194
Revenue deferred from ongoing contractual obligations at fair value		10,384
Deferred tax liability – long-term		2,663
Fair value of assets and liabilities assumed and accrued, net		$ 75,885

We accrued $7.2 million in acquisition related expenses, which included legal and accounting fees, bankers' fees, severance costs and other related costs, of which $342,000, related to severance costs and legal, accounting and tax fees, remains as an accrual as of December 31, 2006.

The following table presents our consolidated results of operations on an unaudited proforma basis as if the acquisitions had taken place at the beginning of the periods presented (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Total revenues	$211,746	$154,591	$130,819
Net loss applicable to common shareholders	(62,900)	(6,732)	(5,018)
Basic and diluted loss per share	$ (0.99)	$ (0.15)	$ (0.11)

The unaudited pro forma data gives effect to actual operating results prior to the acquisitions, and adjustments to reflect interest income foregone, increased intangible amortization, and interest expense for debt assumed. No effect has been given to cost reductions or operating synergies in this presentation. As a result, the unaudited pro forma results of operations are for comparative purposes only and are not necessarily indicative of the results that would have been obtained if the acquisition had occurred as of the beginning of the periods presented or that may occur in the future.

3. Acquisition of CyberGuard

On January 12, 2006, we acquired 100% of the outstanding common shares of CyberGuard Corporation. CyberGuard provided network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication. CyberGuard's products included firewall, Virtual Private Network (VPN), secure content management and security management technologies. This acquisition strengthens our position as one of the market leaders in Network Gateway Security and strengthens our position in the Web Gateway Security space. Additionally, we now have a larger presence in the Global 5000 enterprise markets as well as the U.S. federal government.

The aggregate purchase price was $310.7 million consisting of the issuance of 16.3 million shares of common stock valued at $188.5 million, $2.73 in cash issued for each outstanding share of CyberGuard common stock valued at $88.9 million, the conversion of outstanding CyberGuard stock options into options to purchase 3.0 million shares of our common stock with a value of $29.3 million and direct costs of the acquisition of $4.0 million. The value of the common shares issued was determined based on the average market price of our common shares over the period including two days before and two days after the date that the terms of the acquisition were agreed to and announced. We financed $70.0 million of the CyberGuard acquisition through the issuance of preferred equity securities. See Note 7 for details on the equity financing.

The acquisition was accounted for under the purchase method of accounting, and accordingly, the assets and liabilities acquired were recorded at their estimated fair values at the effective date of the acquisition and the results of operations have been included in the consolidated statements of operations since the acquisition date. In accordance with SFAS No. 142, goodwill and indefinite lived trademarks recorded as a result of the acquisition will be subject to an annual impairment test and will not be amortized.

The following table summarizes the preliminary fair values of the assets acquired and liabilities assumed at the date of acquisition (in thousands):

		As of January 12, 2006
Cash paid, net of cash acquired		$ (69,096)
Current assets		18,067
Property and equipment		2,090
Other long-term and indefinite lived assets		10,570
Goodwill		268,314
Intangible assets subject to amortization:		
Customer relationships (60 month useful life)	28,610	
Tradenames (6 month useful life)	390	
Tradenames (12 month useful life)	290	
Acquired developed technology (12 month useful life)	2,080	
Acquired developed technology (36 month useful life)	1,160	
Acquired developed technology (48 month useful life)	6,930	
		39,460
Total assets acquired		269,405
Current liabilities		9,325
Acquisition reserve		9,358
Revenue deferred from ongoing contractual obligations at fair value		28,903
Deferred tax liability – long-term		4,017
Fair value of assets and liabilities assumed and accrued, net		$217,802

We accrued $9.4 million in acquisition related expenses, which included legal and accounting fees, excess capacity costs, directors and officers insurance policy premium, bankers' fees, severance costs and other costs of which $2.0 remains as an accrual as of December 31, 2006.

EXHIBIT 23

PART 3

The following table presents our consolidated results of operations on an unaudited proforma basis as if the acquisitions had taken place at the beginning of the periods presented (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Total revenues	$178,474	$167,775	$153,118
Net (loss)/income	(27,377)	7,850	1,110
Net (loss)/income applicable to common shareholders	(30,927)	4,197	(2,552)
Basic (loss)/earnings per share	$ (0.54)	$ 0.08	$ (0.05)
Diluted (loss)/earnings per share	$ (0.54)	$ 0.15	$ (0.05)

The unaudited pro forma data gives effect to actual operating results prior to the acquisitions, and adjustments to reflect interest income foregone, increased intangible amortization, income taxes, and preferred stock accretion. No effect has been given to cost reductions or operating synergies in this presentation. As a result, the unaudited pro forma results of operations are for comparative purposes only and are not necessarily indicative of the results that would have been obtained if the acquisition had occurred as of the beginning of the periods presented or that may occur in the future.

4. Investments

Cash Equivalents, Short-Term Investments and Restricted Cash

Our cash equivalents, short-term investments and restricted cash were as follows (in thousands):

	As of December 31,	
	2006	2005
Money market funds	$ 42	$ 32,998
Variable rate demand note	—	4,210
Commercial paper	—	12,920
Federal agencies	—	999
U.S. treasury bills	—	3,963
Taxable auction rate securities	—	22,950
Certificates of deposit	218	245
Total investments	260	78,285
Amounts classified as cash equivalents	—	(47,145)
Restricted cash set aside in bank account	197	—
Total short-term investments and restricted cash	$457	$ 31,140

All short-term investments are debt securities and mature within one year. Unrealized losses on available-for-sale investments at December 31, 2006 and 2005 were none and $2,000, respectively and are reported as a component of other comprehensive (loss)/income in the statement of stockholders' equity. We have restricted cash pledged in the form of certificates of deposit and money market funds against our letters of credit of $205,000 and $40,000, respectively, at December 31, 2006 and in the form of certificates of deposit and money market funds of $240,000 and $40,000, respectively, at December 31, 2005. Interest income on cash equivalents, short-term investments and restricted cash was $2.7 million in 2006, prior to the liquidation of investments and cash equivalents to finance the CipherTrust acquisition, and $1.9 million in 2005.

Equity Investment in a Privately Held Company

As of December 31, 2006, we held an equity investment with a carrying value of $2.7 million in a privately-held company. This investment was recorded at cost as we do not have significant influence over the investee and is classified as other assets on our consolidated balance sheets. This was a related party transaction as discussed in Note 16.

5. Goodwill and Other Intangible Assets

The changes in goodwill during 2006 and 2005 were as follows (in thousands):

Balance as of December 31, 2004	$ 39,329
Reversal of N2H2 reserves	(99)
Balance as of December 31, 2005	$ 39,230
Addition due to CyberGuard acquisition	268,314
Addition due to CipherTrust acquisition	233,857
Recognition of acquired deferred tax assets	(7,742)
Balance as of December 31, 2006	$533,659

As of December 31, 2006, indefinite lived tradenames related to the CipherTrust and CyberGuard acquisitions were $6.9 million and $10.5 million, respectively.

Identified intangible assets subject to amortization are as follows (in thousands):

	As of December 31, 2006			As of December 31, 2005		
	Carrying Value	Accumulated Amortization	Net	Carrying Value	Accumulated Amortization	Net
Customer lists	$44,049	$(10,795)	$33,254	$1,141	$ (840)	$ 301
Tradenames	680	(671)	9	—	—	—
Control lists	771	(660)	111	771	(493)	278
Capitalized developed technology	31,657	(5,904)	25,753	42	(42)	—
Patents and trademarks	1,665	(502)	1,163	1,382	(340)	1,042
Capitalized software	953	(250)	703	452	(259)	193
Total	$79,775	$(18,782)	$60,993	$3,788	$(1,974)	$1,814

Total amortization expense was $17.0 million, $881,000 and $887,000 for the years ended December 31, 2006, 2005 and 2004, respectively. Of the total amortization expense, $187,000, $156,000, and $219,000 pertained to capitalized software costs for the years ended December 31, 2006, 2005, and 2004. Estimated amortization expense for each of the five succeeding fiscal years based on current intangible assets is expected to be $19.1 million, $16.7 million, $14.8 million, $9.1 million and $1.3 million, respectively.

6. Debt

Debt as of December 31, 2006 consists of the following (in thousands):

Secured term loan, due August 31, 2013, LIBOR plus 3.25%	88,000
Deferred financing fees related to secured term loan, due August 31, 2013	(2,977)
Total debt	$85,023

Senior Secured Credit Facility

On August 31, 2006, we entered into a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank. The credit facility provides for a $90.0 million term loan facility, a $20.0 million revolving credit facility, and a swingline loan sub-facility. The proceeds from this transaction were used to finance a portion of the CipherTrust acquisition as noted in Note 2 above. The term loan matures on August 31, 2013 and is payable in 27 scheduled quarterly installments of $225,000 beginning in December 2006 with a final payment of $83.9 million due at maturity. Interest is payable quarterly on the term loan at the London Interbank Offered Rate ("LIBOR") + 3.25%. The interest rate on the term loan may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +3.00%. The interest rate in effect as of December 31,. 2006 was 8.62%. Including amortization of deferred financing fees, we incurred $2.9 million of interest expense in 2006 and none in 2005. Our future payment obligations under this credit facility, are as follows (in thousands):

		Payments Due by Period			
	Total	Less Than One Year	One to Three Years	Three to Five Years	After Five Years
Principal payments on debt	$ 88,000	$ —	$ 925	$ 1,800	$85,275
Interest payments on debt	50,509	7,730	15,365	15,077	12,337
Total	$138,509	$7,730	$16,290	$16,877	$97,612

The revolving credit facility matures on August 31, 2012 with interest payable quarterly at LIBOR + 3.25%. The interest rate on the revolving credit facility may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +2.75%. The revolving credit facility also requires that we pay an annual commitment fee of .5%. The annual commitment fee, based on our Leverage Ratio and ranging from .5% to .375%, is payable quarterly in arrears. The Leverage Ratio is defined as the ratio of (a) consolidated indebtedness to (b) consolidated adjusted EBITDA (earnings before interest, taxes, depreciation, amortization and other adjustments as defined in the agreement). The Leverage Ratio will be calculated quarterly on a pro forma basis that includes the four preceding quarters. The initial Leverage Ratio calculation will be as of December 31, 2006 and cannot exceed the following thresholds over the term of the loan: August 31, 2006 through December 31, 2006 – 4.75 to 1.00; First six months of Fiscal 2007 – 4.00 to 1.00; Last six months of Fiscal 2007 – 3.50 to 1.00; Fiscal 2008 – 2.50 to 1.0; Fiscal 2009 – 2.25 to 1.00; Fiscal 2010 through maturity – 2.00 to 1.00.

The obligations under the senior secured credit facility are guaranteed by us and are secured by a perfected security interest in substantially all of our assets. Financing fees incurred in connection with the credit facility were deferred and are included as a reduction to our long-term debt. These fees are being amortized to interest expense over the term of the term loan using the effective interest rate method.

Debt Covenants

The credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain quarterly financial covenants, beginning with the quarter ended December 31, 2006, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We are in compliance with all covenants as of December 31, 2006.

Derivative Instrument

We have entered into a 3-month LIBOR interest rate cap agreement to cap the interest rate at 5.5% on $60.0 million, or approximately 67% of the aggregate term loan. The notional amount of the agreement decreases $10.0 million each quarter starting March 30, 2007. The agreement terminates on June 30, 2008. The interest rate cap agreement is designated as a cash flow hedge and is reflected at fair value in our consolidated balance sheet. The related gains or losses on this contract are reflected in stockholders' equity as a component of other comprehensive (loss)/income. However, to the extent that this contract is not considered to be perfectly effective in offsetting the change in the value of the item being hedged, any change in fair value relating to the ineffective portion of this contract will be immediately recognized in income. The unrealized gain on the interest rate cap agreement is $19,000 as of December 31, 2006.

7. Equity Financing

On January 12, 2006, we received from Warburg Pincus Private Equity IX, L.P., a global private equity fund, $70.0 million in gross proceeds from the issuance of 700,000 of Series A Convertible Preferred Stock (the preferred stock), a warrant to acquire 1.0 million shares of our common stock and election of a member to our Board of Directors. Based on a quoted market price as of January 12, 2006 and the fair value of the warrant as determined using the Black-Scholes model, we valued the preferred stock at $62.0 million and the warrant at $8.0 million. The proceeds from this transaction were used to finance most of the cash portion of the CyberGuard acquisition as noted in Note 3 above.

On August 31, 2006, the conversion price for the preferred stock was adjusted from the original price of $13.51 to $12.75 per share in accordance with an anti-dilution adjustment triggered by the CipherTrust acquisition. Holders of our preferred stock will be entitled to receive benefits not available to holders of our common stock. These benefits include, but are not limited to, the following: beginning in July 2010, shares of preferred stock will be entitled to receive semi-annual dividends, which may be paid in cash or added to the preferred stock liquidation preference equal to 5% of the preferred stock liquidation preference per year and each share of preferred stock has an initial liquidation preference of $100 which accretes daily at an annual rate of 5%, compounded semi-annually, until July 2010.

On August 31, 2006, the exercise price for the warrant was adjusted from the original price of $14.74 to $13.85 per share also in accordance with an anti-dilution adjustment triggered by the CipherTrust acquisition. The warrant expires on January 12, 2013. When the market price of our common stock is above their exercise price, the warrant becomes dilutive and 1.0 million shares are immediately included in the computation of diluted earnings per share as if the warrant is exercised using the treasury stock method.

The preferred stock was initially reflected on our financial statements at $62.0 million, which is a discount of $8.0 million from its initial liquidation value of $70.0 million due to the fair value of warrants on the effective date. The liquidation value of the preferred stock accretes daily at an annual rate of 5%, compounded semi-annually. This accretion is recorded as a reduction of earnings attributable to common shareholders ratably for a period of 54 months after date of issuance.

We incurred a beneficial conversion charge of $12.6 million, which was recorded as a reduction in earnings attributable to common shareholders in 2006, upon the issuance of the preferred stock since the effective conversion price, after adjusting for the value of the warrants, was less than market price on January 12, 2006, the date of issuance. However, in August 2005 when the terms of the preferred stock issuance to Warburg Pincus in the Securities Purchase Agreement were negotiated, the average market price of the common stock was, in fact, less than the conversion price.

8. Letters of Credit

As of December 31, 2006, we have three letter of credit agreements totaling $247,000. One letter of credit for $205,000 and $240,000, as of December 31, 2006 and 2005, respectively, is with a bank to secure rental space for our San Jose, CA office and automatically renews for a one year period each year through March 31, 2008. Two remaining letters of credit totaling $42,000 and $40,000 as of December 31, 2006 and 2005, respectively, are to secure business with an international customer, which expire May and August 2008.

9. Leases

We lease office space for all of our locations. Renewal options exist for our Concord, CA, and St. Paul, MN offices. Future lease payments for all operating leases, excluding executory costs such as management and maintenance fees and property tax, are as follows (in thousands):

	Future Lease Obligations	Sublease	Net Future Lease Obligations
2007	$ 5,474	$(210)	$ 5,264
2008	4,381	(210)	4,171
2009	3,371	(122)	3,249
2010	2,238	—	2,238
2011	1,957	—	1,957
Thereafter	6,354	—	6,354
	$23,775	$(542)	$23,233

Rent expense including executory costs, net of sublease income was $5.4 million for the year ended December 31, 2006, and $3.9 million for both the years ended December 31, 2005 and 2004. One of our directors and officers is Chairman of the Board of Directors and a majority shareholder in AirDefense, Inc. (AirDefense). In August 2006, we assumed from CipherTrust a sublease agreement with AirDefense, subleasing approximately 13,997 square feet of the 75,288 square feet leased office space located in Alpharetta, GA. For the years ending December 31, 2007, 2008, and 2009 we expect to receive $210,000, $210,000 and $122,000, respectively, from AirDefense according to the terms of the sublease agreement. Sublease income is shown on the consolidated results of operation as a reduction of general and administrative expenses.

10. Share-Based Compensation

Description of Plans

2002 Stock Incentive Plan

Under our 2002 Stock Incentive Plan (2002 Plan), we are permitted to grant incentive and non-qualified stock options, restricted stock awards, restricted stock units, stock appreciation rights and other similar types of stock awards, such as phantom stock rights, to our employees and non-employee directors. There were a total of 6.5 million shares authorized under the 2002 Plan at December 31, 2006. All options granted under the 2002 Plan through December 31, 2006 have exercise prices equal to the fair market value of our stock on the date of grant. Options granted under the 2002 Plan have ten-year terms and typically vest 25% after the first year and then monthly over the following three years. All awards granted to non-employee directors vest 100% after the first year. Outstanding awards that were originally granted under several predecessor plans also remain in effect in accordance with their terms. Restricted stock awards vest 25% after the first year, then quarterly thereafter over the following three years, unless otherwise approved by the Compensation Committee.

1995 Omnibus Stock Option Plan

In September 1995, our Board of Directors and stockholders approved our 1995 Omnibus Stock Plan. The majority of options granted under this plan had ten year terms and vested either annually over three years, or fully vested at the end of three years. Beginning in 2003, all new stock options granted under this plan vest 25% after the first year and then monthly over the following three years. This plan expired in September 2005. As of December 31, 2006, there were 5.1 million options outstanding under this Plan, of which 380,283 were not yet vested.

N2H2 Stock Option Plans

In connection with our acquisition of N2H2 in October 2003, we assumed all of the outstanding N2H2 stock options under the 1997 Stock Option Plan, 1999 Stock Option Plan, 1999 Non-Employee Director Plan, 1999/2000 Transition Plan, the 2000 Stock Option Plan, and the Howard Philip Welt Plan, which were converted into options to purchase approximately 420,000 shares of our common stock. All stock options assumed were exercisable and vested. These options were assumed at prices between $1.55 and $258.63 per share, with a weighted average exercise price of $10.06 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

CyberGuard Stock Option Plans

In connection with our acquisition of CyberGuard in January 2006, we assumed all of the outstanding CyberGuard stock options under the 1994 and 1998 Stock Option Plans which were converted into options to purchase 3,039,545 shares of our common stock. All outstanding stock options assumed were exercisable and vested. These options were assumed at prices between $1.56 and $15.07 per share, with a weighted average exercise price of $7.21 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

CipherTrust 2000 Stock Option Plan

In connection with our acquisition of CipherTrust in August 2006, we assumed all of the outstanding CipherTrust stock options under the 2000 Stock Option Plan which were converted into 2,543,662 shares of our common stock. All outstanding stock options assumed were unvested and have seven-year terms. These options were assumed at prices between $0.01 and $6.19 per share, with a weighted average exercise price of $2.88 per share. The options granted under this plan, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

Employee Stock Purchase Plan

We have an employee stock purchase plan (ESPP), which enables employees to contribute up to 10% of their compensation toward the purchase of our common stock at the end of the participation period at a purchase price equal to 85% of the lower of the fair market value of the common stock on the first or last day of the participation period. For the fourth quarter of 2006 and the first quarter of 2007, the Board of Directors and the Compensation Committee have approved to increase the maximum contribution up to 20% of compensation. Common stock reserved for future employee purchases under the plan totals 589,534 shares at December 31, 2006. Common stock issued under the plan totaled approximately 279,000 in 2006, 164,000 in 2005 and 165,000 in 2004.

Impact of the Adoption of SFAS No. 123(R)

See Note 1 for a description of our adoption of SFAS No. 123(R), on January 1, 2006. A summary of the share-based compensation expense that we recorded in accordance with SFAS No. 123(R) for the twelve months ended December 31, 2006 for stock options, restricted stock and shares purchased under our ESPP is as follows (in thousands, except per share amounts):

	Year Ended December 31, 2006
Cost of product revenues	$ 357
Cost of service revenues	567
Selling and marketing	5,260
Research and development	2,542
General and administrative	1,830
Increase of loss before income taxes	$10,556
Increase of basic loss per share	$ (0.19)

Prior to the adoption of SFAS No. 123(R), we presented all tax benefits for deductions resulting from the exercise of stock options as operating cash flows on our statement of cash flows. SFAS No. 123(R) requires the cash flows resulting from the tax benefits for tax deductions in excess of the compensation expense recorded for those options (excess tax benefits) to be classified as financing cash flows. There were no excess tax benefits for the year ended December 31, 2006.

Determining Fair Value

Valuation and Amortization Method. We estimate the fair value of stock options granted using the Black-Scholes option valuation model. For options granted before January 1, 2006, we amortize the fair value on an accelerated basis. For options granted on or after January 1, 2006, we amortize the fair value on a straight-line basis. All options are amortized over the requisite service periods of the awards, which are generally the vesting periods. For restricted stock, the fair value is calculated as the market price on date of grant and we amortize the fair value on a straight-line basis over the requisite service period of the award, which is generally the vesting period.

Expected Term. The expected term of options granted represents the period of time that they are expected to be outstanding. In light of new accounting guidance under SFAS No. 123(R) and SAB No. 107, we reevaluated our expected term assumption used in estimating the fair value of employee options. We estimate the expected term of options granted based on historical exercise patterns, which we believe are representative of future behavior. Our estimate of the expected life of new options granted to our employees is 3 years, consistent with prior periods. We have examined our historical pattern of option exercises in an effort to determine if there were any discernable patterns of activity based on certain demographic characteristics. Demographic characteristics tested included age, salary level, job level and geographic location. We have determined that there were no meaningful differences in option exercise activity based on the demographic characteristics tested.

Expected Volatility. Also in light of implementing SFAS No. 123(R), we reevaluated our expected volatility assumption used in estimating the fair value of employee options. We estimate the volatility of our common stock at the date of grant based on historical volatility, consistent with SFAS No. 123(R) and SAB No. 107. Our decision to use historical volatility instead of implied volatility was based upon analyzing historical data along with the lack of availability of history of actively traded options on our common stock.

Risk-Free Interest Rate. We base the risk-free interest rate that we use in the Black-Scholes option valuation model on the implied yield in effect at the time of option grant on U.S. Treasury zero-coupon issues with equivalent remaining terms.

Dividends. We have never paid cash dividends on our common stock and we do not anticipate paying cash dividends in the foreseeable future. Consequently, we use an expected dividend yield of zero in the Black-Scholes option valuation model.

Forfeitures. SFAS No. 123(R) requires us to estimate forfeitures at the time of grant and revise those estimates in subsequent periods if actual forfeitures differ from those estimates. We use historical data to estimate pre-vesting option forfeitures and record share-based compensation expense only for those awards that are expected to vest. For purposes of calculating pro forma information under SFAS No. 123 for periods prior to 2006, we accounted for forfeitures as they occurred.

We used the following assumptions to estimate the fair value of options granted and shares purchased under our ESPP for the twelve months ended December 31, 2006, 2005 and 2004, respectively:

	Year Ended December 31,		
	2006	2005	2004
Stock Options – Assumptions used:			
Average expected terms (years)	3	3	5
Weighted-average volatility	83.0%	85.0%	97.0%
Risk-free interest rate	4.8%	3.9%	3.6%
Dividend yield	0%	0%	0%
ESPP – Assumptions used:			
Average expected terms (years)	0.25	0.25	0.25
Weighted-average volatility	56.5%	48.8%	74.4%
Risk-free interest rate	4.6%	3.2%	1.4%
Dividend yield	0%	0%	0%

The Black-Scholes option-pricing model was developed for use in estimating the fair value of traded options that have no vesting restrictions and are fully transferable. In addition, option valuation models require the input of highly subjective assumptions, including the expected stock price volatility. Because changes in the subjective input assumptions can materially affect the fair value estimate, in our opinion, the existing models do not necessarily provide a reliable single value of our options and may not be representative of the future effects on reported net income or loss or the future stock price of our company.

Share-Based Compensation Expense and Stock Option Activity

For the year ended December 31, 2006, we recorded $10.6 million in share-based compensation expense, which includes $9.4 million for stock options, $529,000 for our ESPP and $637,000 for restricted stock. At December 31, 2006, we had 373,000 non-vested restricted stock awards that had a weighted average grant date fair value of $9.80. As of December 31, 2006, there was $32.7 million of total unrecognized compensation cost related to non-vested share-based compensation arrangements granted under all equity compensation plans. Total unrecognized compensation cost will be adjusted for future changes in estimated forfeitures. We expect to recognize that cost over a weighted average period of 3.1 years.

A summary of stock option activity under all stock plans during the year ended December 31, 2006 is as follows:

	Stock Options	Weighted Average Exercise Price per Share	Weighted Average Remaining Contractual Life (Years)	Aggregate Intrinsic Value
Outstanding at December 31, 2005	8,549,315	$10.06	6.5	$18,793,738
Granted	4,614,199	8.28	9.8	—
Assumed upon acquisition of CyberGuard	3,039,545	7.21	3.5	—
Assumed upon acquisition of CipherTrust	2,543,662	2.88	2.6	—
Exercised	(1,418,544)	4.51	—	7,934,248
Cancelled/forfeited/expired	(1,467,625)	8.58	—	—
Outstanding at December 31, 2006	15,860,552	8.52	6.6	11,608,819
Shares vested and expected to vest	15,064,588	8.97	6.8	11,585,629
Exercisable at December 31, 2006	8,637,863	$ 9.45	5.2	$ 6,172,481

We define in-the-money options at December 31, 2006 as options that had exercise prices that were lower than the $6.56 market price of our common stock at that date. The aggregate intrinsic value of options outstanding at December 31, 2006 is calculated as the difference between the exercise price of the underlying options and the market price of our common stock for the 4.0 million shares that were in-the-money at that date. There were 2.1 million in-the-money options exercisable at December 31, 2006. During the year ended December 31, 2006, 373,000 shares of restricted stock were awarded to employees and directors, of which none had vested as of December 31, 2006. There were no restricted stock awards prior to 2006.

We received $6.4 million in cash from option exercises under all share-based payment arrangements for the year ended December 31, 2006.

Comparable Disclosure

Prior to January 1, 2006, we accounted for our share-based compensation plans under the recognition and measurement provisions of APB Opinion No. 25 and related Interpretations. No share-based employee compensation cost is reflected in the condensed consolidated statements of operations for the years ended December 31, 2005 and 2004, as all options granted under those plans had an exercise price equal to the market value of the underlying common stock on the date of grant. The following table illustrates the effect on net income and net income per share if we had applied the fair value recognition provisions of SFAS No. 123 to share-based employee compensation prior to January 1, 2006 (in thousands, except per share amounts):

	Year Ended December 31,	
	2005	2004
Net income, as reported	$ 21,374	$ 12,835
Deduct: Total stock-based employee compensation expense determined under fair value based method for all awards, net of related tax effects	(10,454)	(11,728)
Pro forma net income	$ 10,920	$ 1,107
Net income per share:		
Basic – as reported	$ 0.59	$ 0.36
Basic – pro forma	$ 0.30	$ 0.03
Diluted – as reported	$ 0.57	$ 0.34
Diluted – pro forma	$ 0.29	$ 0.03

11. Defined Contribution Plans

We have a voluntary defined contribution plan under Section 401(k) of the Internal Revenue Code that covers substantially all U.S. employees. Through 2006 the 401(k) plan provided a discretionary year-end employer matching contribution on employee deferral contributions made during the plan year. The employer matching contribution will be made quarterly in 2007. Employer contributions made to the 401(k) plan were $401,000 during 2006, $274,000 during 2005, and none during 2004.

12. Income Taxes

For financial reporting purposes, (loss) income before income taxes includes the following components (in thousands):

	Year Ended December 31,		
	2006	2005	2004
(Loss) income before income taxes:			
U.S.	$(19,747)	$21,425	$12,352
Non U.S. subsidiaries	1,854	557	483
Total (loss) income before income taxes	$(17,893)	$21,982	$12,835

During 2006, we recorded income tax expense of $9.5 million. Of this $9.5 million income tax expense, a non-cash expense of $8.5 million is related to a net tax valuation allowance recorded on our net deferred tax assets. We were unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses, and needed to provide tax expense for the subsequent valuation allowance reapplied to the remaining net operating losses. This was a result of changes in circumstances due to recent acquisitions that caused a change in judgment regarding the realizability of our net deferred tax assets in the fourth quarter. The remainder of the income tax expense is related to current income tax components such as, alternative minimum income tax, and state and foreign income taxes. This is compared with $608,000 of income tax expense recorded in 2005 which consisted of $349,000 for alternative minimum tax expense, $58,000 for state income tax expense and $201,000 for various foreign income tax expenses.

Federal alternative minimum tax was provided on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carryforward which we have available. Similar to 2006, we anticipate that we will be in an alternative minimum taxable income position in 2007. Current tax law provides that part or all of the amount of the alternative minimum tax paid can be carried forward indefinitely and credited against federal regular tax in future tax years to the extent the regular tax liability exceeds the alternative minimum tax in those years. For 2006, the reversal of $3.1 million of the tax valuation allowance related to acquired net operating losses was recorded as a decrease to goodwill in the balance sheet and not as a benefit to tax expense in the income statement.

The components for the provision for income taxes were as follows (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Current income tax expense:			
U.S.	$ 465	$349	$ —
States (U.S.)	212	58	62
Non U.S. subsidiaries	644	201	283
Deferred income tax expense:			
U.S.	7,459	—	(345)
States (U.S.)	725	—	—
Non U.S. subsidiaries	—	—	—
Total income tax expense	$9,505	$608	$ —

A reconciliation of our provision for income taxes to the statutory tax rate based upon pretax (loss) income was as follows (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Income taxes at U.S. statutory tax rate	$ (6,262)	$ 7,739	$ 4,264
State taxes, net of federal benefit	(137)	734	249
Non U.S. tax rate differential	(310)	6	203
Change in valuation allowance	12,870	(10,543)	(4,663)
Change in deferred tax rate	—	3,066	—
Change in tax credit carryforwards	—	(360)	—
Stock-based compensation	2,257	—	—
Imputed income	623	—	—
Other	464	(34)	(53)
Total income tax expense	$ 9,505	$ 608	$ —

Deferred income tax assets and liabilities result from temporary differences between the carrying values of assets and liabilities for financial statement and income tax purposes. Significant components of our net deferred tax assets and liabilities are as follows (in thousands):

	As of December 31,		
	2006	2005	2004
Deferred tax assets:			
Accrued liabilities	$ 1,104	$ 538	$ 1,086
Payroll liabilities	638	363	239
Tax assets over book assets	3,956	—	—
Tax over book amortization	1,861	(864)	(612)
Book over tax depreciation	—	619	93
Deferred revenue	4,164	2,034	—
Stock compensation	1,188	—	—
Income tax credits	1,095	838	478
Net operating loss carryforward	110,603	68,236	79,172
Total deferred tax assets before valuation allowance	124,609	71,764	80,456
Less valuation allowance	(100,225)	(68,160)	(76,852)
Net deferred tax assets after valuation allowance	24,384	3,604	3,604
Deferred tax liabilities:			
Acquired indefinite lived intangibles	7,672	—	—
Acquired definite lived intangibles	22,724	—	—
Other deferred tax liabilities	1,660	—	—
Total deferred tax liabilities	32,056	—	—
Net deferred tax (liabilities) assets	$ (7,672)	$ 3,604	$ 3,604

In accordance with SFAS No. 109, we have assessed the likelihood that the net deferred tax assets will be realized. SFAS No. 109, "Accounting for Income Taxes," requires the consideration of a valuation allowance in all circumstances, if the conclusion is not more likely than not a valuation allowance is required. We have determined that it is more likely than not that deferred tax assets of $24.4 million at December 31, 2006 will be realized based on our expected future reversals of certain deferred tax liabilities. We have a net deferred tax liability recorded in our balance sheet that consists primarily of indefinite lived intangible assets that are not deductible for tax purposes and therefore cannot be used to realize additional reversing deferred tax assets. In accordance with SFAS No. 109, our remaining noncurrent deferred tax liabilities are netted with our noncurrent deferred tax assets and are presented as a single amount in our consolidated balance sheet.

Worldwide net operating loss carryforwards totaled approximately $479.5 million at December 31, 2006, comprised of $456.6 million domestic net operating loss carryforwards and $22.9 million of international net operating loss carryforwards. These carryforwards are available to offset taxable income through 2026 and will start to expire in 2011. Of these carryforwards, $208.1 million relates to acquired CyberGuard net operating losses, $59.6 million relates to acquired N2H2 net operating losses, and $19.4 million relates to acquired CipherTrust net operating losses. We have provided a complete valuation allowance on primarily all of these acquired losses are fully valued against, and upon release of the valuation allowance, a portion of the benefit will go to the balance sheet to reduce goodwill instead of a benefit to the income tax provision. As of December 31, 2006 we have deducted $56.8 million related to stock option exercises. The tax benefit in excess of book expense from these stock option exercises will be recorded as an increase to additional paid-in capital upon utilization of the net operating losses under the financial statement approach to recognizing the tax benefits associated with stock option deductions. Of the remaining benefit associated with the carryforwards, approximately $111.3 million has yet to be recognized in the consolidated statement of operations. However, there are no assurances that the tax benefit of these carryforwards will be available to offset future income tax expense when taxable income is realized.

Nò provision has been made for U.S. federal income taxes on certain cumulative undistributed earnings of non U.S. subsidiaries as we intend to indefinitely reinvest these earnings in the non U.S. subsidiaries or the earnings may be remitted substantially tax-free. The total cumulative undistributed earnings of certain of our non U.S. subsidiaries that would be subject to federal income tax if remitted under existing law is approximately $5.9 million at December 31, 2006. Determination of the unrecognized deferred tax liability related to these earnings is not practicable because of the complexities with its hypothetical calculation. Upon distribution of these earnings, we may be subject to U.S. taxes and withholding taxes payable to various foreign governments.

13. Contingencies

In December 2002, we were named as the defendant in a rental property lawsuit brought by Salvio Pacheco Square LLP in the Superior Court of California, County of Contra Costa. The complaint alleges that we breached a commercial lease at our Concord, CA office and asked for declaratory relief, and compensatory and other damages. The Superior Court entered judgment in favor of plaintiff in June 2004 in the amount of $1.1 million and found we had breached the lease. We appealed to the First Appellate District, California Court of Appeal. The Court of Appeal denied our appeal in April 2006. In addition to the judgment entered by the Superior Court in June 2004, we incurred additional costs of $1.4 million as damages for the rental and other costs due on the balance of the lease, interest on the judgment and unpaid amounts due under the lease and plaintiff's attorney's fees and costs. As a result of the April 2006 denial of our appeal, we accrued $2.5 million as of March 31, 2006 for the settlement of this litigation. The settlement of $2.5 million was subsequently paid in July 2006.

On June 5, 2006, Finjan Software, Ltd. filed a complaint entitled Finjan Software, Ltd. v. Secure Computing Corporation in the United States District Court for the District of Delaware against Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG. The complaint alleges that Secure Computing and its named subsidiaries infringe U.S. Patent No. 6,092,194 ("'194 Patent") based on the manufacture, use, and sale of the Webwasher Secure Content Management suite. Secure Computing denies infringing any valid claims of the '194 Patent. The answer to the complaint was filed on July 26, 2006. Discovery is proceeding.

On January 19, 2007, Rosenbaum Capital, LLC filed a putative securities class action complaint in the United States District Court for the Northern District of California against us and certain directors and officers of the company. The alleged plaintiff class includes persons who acquired stock between May 4, 2006 through July 11, 2006. The complaint alleges generally that defendants made false and misleading statements about our business condition and prospects for the fiscal quarter ended June 30, 2006, in violation of Section 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. The complaint seeks unspecified monetary damages. While there can be no assurance as to the outcome of this or any other litigation we believe there are meritorious legal and factual defenses to this action and we intend to defend ourselves vigorously.

From time to time we may be engaged in certain other legal proceedings and claims arising in the ordinary course of our business. The ultimate liabilities, if any, which may result from these or other pending or threatened legal actions against us cannot be determined at this time. However, in the opinion of management, the facts known at the present time do not indicate that such litigation will have a material effect on our consolidated financial position or results of operation.

14. Net (Loss)/Income Per Share

The following table represents the calculation of basic and diluted net (loss)/income per share (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Net (loss)/income applicable to common stockholders	$(43,551)	$21,374	$12,835
Shares used in computing basic net (loss)/income per share	57,010	36,338	35,576
Outstanding dilutive stock options	—	1,371	1,680
Shares used in computing diluted net (loss)/income per share	57,010	37,709	37,256
Basic net (loss)/income per share	$ (0.76)	$ 0.59	$ 0.36
Diluted net (loss)/income per share	$ (0.76)	$ 0.57	$ 0.34

All potential common share equivalents for the year ended December 31, 2006 were excluded from the computation of diluted earnings per share as inclusion of these shares would have been anti-dilutive. Additionally, 5.6 million shares of common stock as if our preferred stock was converted, were excluded from the effect of dilutive securities for the year ended December 31, 2006, because we reported a net loss for this period. Potential common shares of 2.6 million and 2.5 million related to our outstanding stock options were excluded from the computation of diluted earnings per share for 2005 and 2004, respectively, as inclusion of these shares would have been anti-dilutive.

15. Segment Information

We view our operations and manage our business as one segment called enterprise gateway security. Major foreign markets for our products and services include Europe, Japan, China, the Pacific Rim, and Latin America. In each market, we have independent channel partners who are responsible for marketing, selling and supporting our products and services to resellers and end-users within their defined territories. International sales accounted for 39%, 38% and 31% of total revenue for the years 2006, 2005 and 2004, respectively.

The following table summarizes our domestic and international revenues (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Revenues:			
Domestic	$108,547	$ 67,689	$64,431
International	68,150	41,486	28,947
	$176,697	$109,175	$93,378

No customer accounted for more than 10% of our total revenue in 2006, 2005 or 2004.

16. Related Party Transaction

In February 2005, we made a strategic investment in a privately-held technology company. As a result of this $2.7 million investment, we have a 15% ownership stake in this company. This investment is reported in other assets on our consolidated balance sheets and is evaluated for impairment annually.

Two of our board members, one of whom is a board member of the investee, are individual investors of the investee. Due to their involvement with the investee, these two board members recused themselves from our decision to make the investment.

17. Summarized Quarterly Financial Information (unaudited)

	Quarter Ended (in thousands, except per share data)			
	March 31,	June 30,	September 30,	December 31,
2006				
Revenue	$ 42,617	$38,746	$43,748	$ 51,586
Gross profit	30,685	28,822	31,963	36,069
Operating income/(loss) (1)	769	(2,710)	(6,347)	(9,485)
Net income/(loss) (2)	657	6,659	(7,291)	(27,423)
Net (loss)/income applicable to common shareholders	(12,759)	5,722	(8,194)	(28,320)
Basic and diluted (loss)/income per share	$ (0.25)	$ 0.11	$ (0.14)	$ (0.44)
2005				
Revenue	$ 25,579	$26,113	$27,249	$ 30,234
Gross profit	20,594	21,578	22,217	22,737
Operating income	4,121	4,746	5,404	6,080
Net income	4,062	4,946	5,792	6,574
Basic income per share	$ 0.11	$ 0.14	$ 0.16	$ 0.18
Diluted income per share	$ 0.11	$ 0.13	$ 0.15	$ 0.17

(1) Operating loss for the quarter ended June 30, 2006 was negatively impacted by the reduction in revenue recognized in that quarter. For the quarters ended September 30, 2006 and December 31, 2006, operating loss was impacted by the acquisition of CipherTrust. Because we are unable to establish VSOE of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred, while the operating expenses continue to be recognized in the current periods, resulting in a net operating loss impact.

(2) Net income for the quarter ended June 30, 2006 included the impact of benefiting from the reversal of $7.3 million of valuation allowance that had been established against our deferred tax assets. Net loss for the quarter ended December 31, 2006 included a net $15.5 million tax expense due to being unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses and an increase in the valuation allowance established against our deferred tax assets.

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of Secure Computing Corporation

We have audited the accompanying consolidated balance sheets of Secure Computing Corporation as of December 31, 2006 and 2005, and the related consolidated statements of operations, stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2006. Our audits also included the financial statement schedule listed in the Index at Item 15(a). These consolidated financial statements and schedule are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and schedule based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the consolidated financial position of Secure Computing Corporation at December 31, 2006 and 2005, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2006, in conformity with U.S. generally accepted accounting principles. Also, in our opinion, the related financial statement schedule, when considered in relation to the basic consolidated financial statements taken as a whole, presents fairly in all material respects the information set forth therein.

As discussed in Note 1, Summary of Significant Accounting Policies, to the consolidated financial statements, effective January 1, 2006, the Company adopted Statement of Financial Accounting Standards No. 123 (revised 2004), Share-Based Payment, using the modified prospective method.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the effectiveness of Secure Computing Corporation's internal control over financial reporting as of December 31, 2006, based on criteria established in *Internal Control—Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission, and our report dated March 15, 2007, expressed an unqualified opinion on management's assessment and an adverse opinion on the effectiveness of internal control over financial reporting.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of Secure Computing Corporation

We have audited management's assessment, included in the section in Item 9A entitled Management's Report on Internal Control Over Financial Reporting, that Secure Computing Corporation did not maintain effective internal control over financial reporting as of December 31, 2006, because of the effect of ineffective controls over the calculation of income taxes, based on criteria established in *Internal Control—Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). Secure Computing Corporation's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assessment and an opinion on the effectiveness of the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies and procedures may deteriorate.

A material weakness is a control deficiency, or combination of control deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. A material weakness has been identified and described in management's assessment related to an ineffective control over the accounting for income taxes as evidenced by a failure to detect necessary adjustments to the income tax accounts. This deficiency resulted in material adjustments being made to the annual financial statements and rises to the level of a material weakness. This material weakness was considered in determining the nature, timing, and extent of audit tests applied in our audit of the 2006 financial statements, and this report does not affect our report dated March 15, 2007 on those financial statements.

As indicated in the accompanying Management's Report on Internal Control Over Financial Reporting, management's assessment of and conclusion on the effectiveness of internal control over financial reporting did not include the internal controls of the business operations of CipherTrust, Inc. which are included in the 2006 consolidated financial statements of Secure Computing Corporation and constituted approximately $66.0 million and $19.1 million of total and net assets, respectively, as of December 31, 2006 and $7.1 million of revenues for the year then ended. Our audit of internal control over financial reporting of Secure Computing Corporation also did not include an evaluation of the internal control over financial reporting of the business operations of CipherTrust, Inc.

In our opinion, management's assessment that Secure Computing Corporation did not maintain effective internal control over financial reporting as of December 31, 2006, is fairly stated, in all material respects, based on the COSO criteria. Also, in our opinion, because of the material weakness described above on the achievement of objectives of the control criteria, Secure Computing Corporation has not maintained effective internal control over financial reporting as of December 31, 2006, based on the COSO criteria.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007

SECURE COMPUTING CORPORATION

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, as amended, the Registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

SECURE COMPUTING CORPORATION

Date: March 16, 2007

By: /s/ JOHN E. MCNULTY

John E. McNulty
Chairman, President and Chief Executive Officer

Power of Attorney

KNOW ALL MEN BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints John McNulty and Timothy Steinkopf or either of them, his or her true and lawful attorneys-in-fact and agents, with full power of substitution and re-substitution, for him or her and in his or her name, place and stead, in any and all capacities to sign any and all amendments to this Report on Form 10-K, and to file the same, with all exhibits thereto and other documents in connection therewith, with the Securities and Exchange Commission, granting unto the attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that the attorneys-in-fact and agents, or either of them, or their, his or her substitutes or substitute, may lawfully do or cause to be done by virtue hereof.

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed by the following persons on behalf of the Registrant and in the capacities indicated on March 16, 2007.

Signature	Title
/s/ John E. McNulty John E. McNulty	Chairman, President and Chief Executive Officer (Principal Executive Officer)
/s/ Timothy J. Steinkopf Timothy J. Steinkopf	Senior Vice President of Operations and Chief Financial Officer (Principal Financial and Accounting Officer)
/s/ Jay S. Chaudhry Jay S. Chaudhry	Vice Chairman and Chief Strategy Officer
/s/ Robert J. Frankenberg Robert J. Frankenberg	Director
/s/ James F. Jordan James F. Jordan	Director
/s/ Stephen M. Puricelli Stephen M. Puricelli	Director
/s/ Eric P. Rundquist Eric P. Rundquist	Director
/s/ Alexander Zakupowsky, Jr. Alexander Zakupowsky, Jr.	Director
/s/ Cary Davis Cary Davis	Director
/s/ Richard Scott Richard Scott	Director

SCHEDULE II
VALUATION AND QUALIFYING ACCOUNTS
YEARS ENDED DECEMBER 31, 2006, 2005 AND 2004

Description	Balance at Beginning of Year	Additions Charged to Bad Debt Expense	Adjustments to Goodwill	Deductions-Write-offs	Balance at End of Year
Year ended December 31, 2006:					
Allowance for doubtful accounts (1)	$272,000	$947,000	$ 802,000	$(594,000)	$1,427,000
Year ended December 31, 2005:					
Allowance for doubtful accounts	$450,000	$ 69,000	$ —	$(247,000)	$ 272,000
Year ended December 31, 2004:					
Allowance for doubtful accounts (2)	$868,000	$212,000	$(320,000)	$(310,000)	$ 450,000

(1) The amount noted as an adjustment to goodwill reflects the balance of acquired CipherTrust receivables outstanding that are fully reserved as of December 31, 2006.

(2) The amount noted as an adjustment to goodwill reflects the finalization of the purchased N2H2 receivables and therefore, did not impact earnings.

Exhibit 23.1

Consent of Independent Registered Public Accounting Firm

We consent to the incorporation by reference in the Registration Statements on Form S-3 (Nos. 333-132130 and 333-138826) and in the Registration Statements on Form S-8 (Nos. 333-06563, 333-11451, 333-28927, 333-28929, 333-35651, 333-71913, 333-80065, 333-80963, 333-103595, 333-109755, 333-115583, 333-131144 and 333-138828) of our reports dated March 15, 2007, with respect to the consolidated financial statements and schedule of Secure Computing Corporation, Secure Computing Corporation management's assessment of the effectiveness of internal control over financial reporting, and the effectiveness of internal control over financial reporting of Secure Computing Corporation, included in this Annual Report (Form 10-K) for the year ended December 31, 2006.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007

Exhibit 31.1

CERTIFICATION OF CHIEF EXECUTIVE OFFICER PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002

I, John E. McNulty, certify that:

1. I have reviewed this Form 10-K of Secure Computing Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this quarterly report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officers and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and we have:

a) designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b) designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c) evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d) disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting;

5. The registrant's other certifying officers and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of registrant's board of directors (or persons performing the equivalent function):

a) all significant deficiencies in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b) any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

/s/ JOHN E. MCNULTY

John E. McNulty
Chairman, President and Chief Executive Officer

March 16, 2007

Exhibit 31.2

CERTIFICATION OF CHIEF FINANCIAL OFFICER
PURSUANT TO SECTION 302
OF THE SARBANES-OXLEY ACT OF 2002

I, Timothy J. Steinkopf, certify that:

1. I have reviewed this Form 10-K of Secure Computing Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this quarterly report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;

4. The registrant's other certifying officers and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and we have:

a) designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

b) designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

c) evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

d) disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting.

5. The registrant's other certifying officers and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of registrant's board of directors (or persons performing the equivalent function):

a) all significant deficiencies in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

b) any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

/s/ TIMOTHY J. STEINKOPF

Timothy J. Steinkopf
Senior Vice President of Operations and Chief Financial Officer

March 16, 2007

Exhibit 32.1

CERTIFICATION PURSUANT TO 18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

In connection with the Annual Report of Secure Computing Corporation (the "Company") on Form 10-K for the period ending December 31, 2006 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), I, John E. McNulty, Chief Executive Officer of the Company, certify, pursuant to 18 U.S.C. § 1350, as adopted pursuant to § 906 of the Sarbanes-Oxley Act of 2002, that:

(1) The Report fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act of 1934; and

(2) The information contained in the Report fairly presents, in all material respects, the financial condition and result of operations of the Company.

/s/ JOHN E. MCNULTY

John E. McNulty
Chairman, President and Chief Executive Officer

March 16, 2007

Exhibit 32.2

CERTIFICATION PURSUANT TO 18 U.S.C. SECTION 1350, AS ADOPTED PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

In connection with the Annual Report of Secure Computing Corporation (the "Company") on Form 10-K for the period ending December 31, 2006 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), I, Timothy J. Steinkopf, Chief Financial Officer of the Company, certify, pursuant to 18 U.S.C. § 1350, as adopted pursuant to § 906 of the Sarbanes-Oxley Act of 2002, that:

(1) The Report fully complies with the requirements of section 13(a) or 15(d) of the Securities Exchange Act of 1934; and

(2) The information contained in the Report fairly presents, in all material respects, the financial condition and result of operations of the Company.

/s/ TIMOTHY J. STEINKOPF

Timothy J. Steinkopf
Senior Vice President of Operations and Chief Financial Officer

March 16, 2007

BOARD OF DIRECTORS

John McNulty
Chairman of the Board,
President; and CEO

Jay Chaudhry
Vice Chairman and
Chief Strategy Officer

Robert J. Frankenberg
President and Founder,
NetVentures

James F. Jordan
Private Investor

Stephen M. Puricelli
Private Investor

Eric P. Rundquist
Former President and CEO
Eric Thomas Inc.

Alexander Zakupowsky, Jr.
Attorney at Law
Winston & Strawn LLP.

Cary J. Davis
Managing Director
Warburg Pincus

Richard L. Scott
Chairman and CEO
Richard L. Scott Investments, LLC.

EXECUTIVE OFFICERS

John McNulty
Chairman of the Board,
President, and CEO

Jay Chaudhry
Vice Chairman and
Chief Strategy Officer

Tim Steinkopf
Senior Vice President, Operations
and Chief Financial Officer

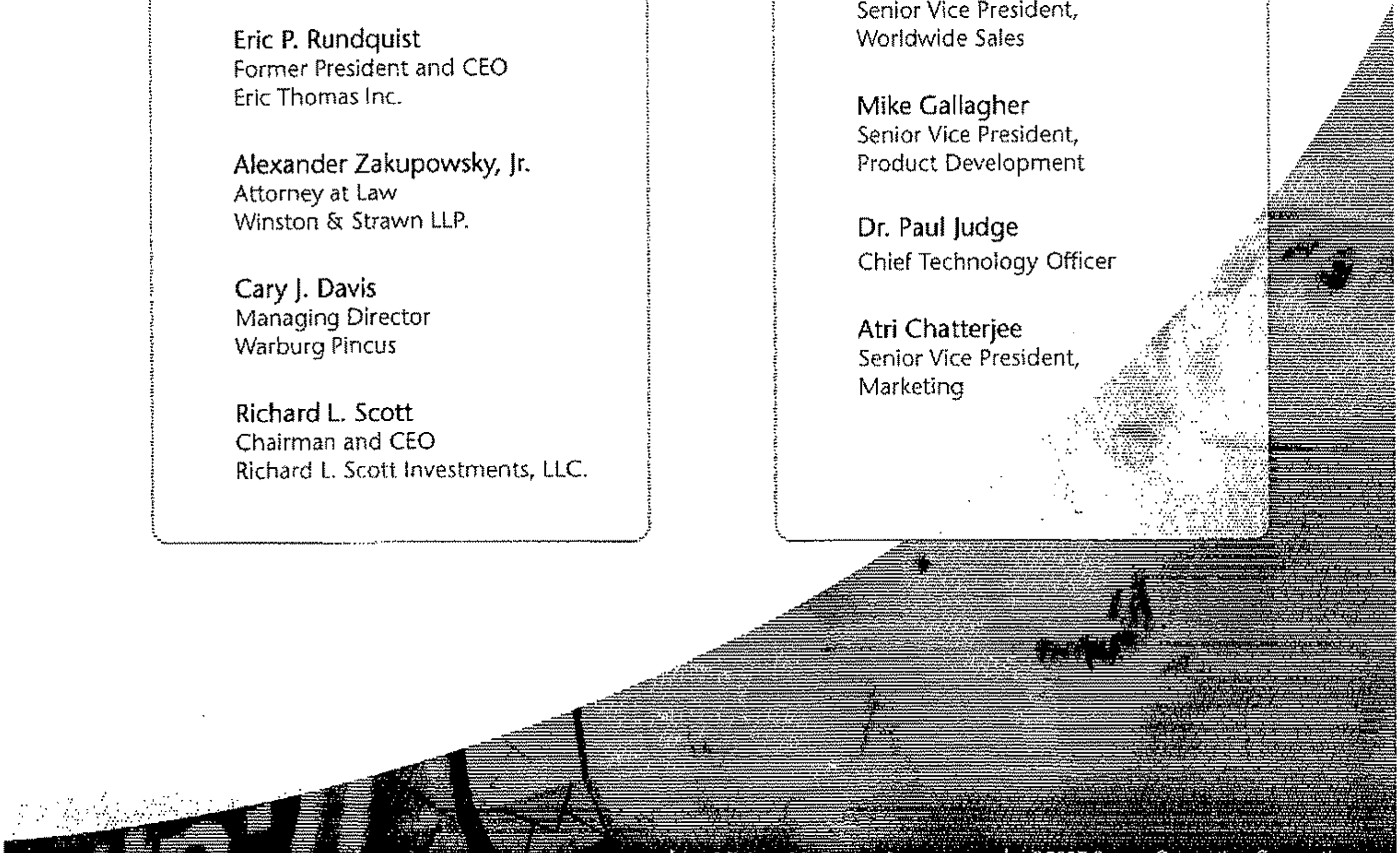
Mary K. Budge
Senior Vice President,
Secretary and General Counsel

Vincent M. Schiavo
Senior Vice President,
Worldwide Sales

Mike Gallagher
Senior Vice President,
Product Development

Dr. Paul Judge
Chief Technology Officer

Atri Chatterjee
Senior Vice President,
Marketing



Registrar and Transfer Agent
Wells Fargo Bank Minnesota, N.A.
Shareowner Services
161 North Concord Exchange
South St. Paul, Minnesota
55075-0738
+1.651.450.4023

Annual Meeting
The 2007 annual meeting of stockholders will be held on Thursday, May 10, 2007 at 10:00 a.m. Pacific Daylight Time, at the Pruneyard Inn,
1995 South Bascom Avenue,
Campbell, California 95008

Additional Information
To request a copy of the Annual Report or Form 10-K please contact:
Investor Relations
Secure Computing Corporation
4810 Harwood Road
San Jose, CA 95124
+1.408.979.6100

SECURE
COMPUTING®

www.securecomputing.com

Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100

European Headquarters
Berkshire, UK
Tel +44.0.870.460.4766

Asia/Pac Headquarters
Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters
Tokyo, Japan
Tel +81.3.5339.6310

EXHIBIT 24
PART 1

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

MARKET ANALYSIS

Worldwide Secure Content Management 2005–2009 Forecast Update and 2004 Vendor Shares: Spyware, Spam, and Malicious Code Continue to Wreak Havoc

Brian E. Burke Rose Ryan

IDC OPINION

The worldwide secure content management (SCM) market grew to $4.5 billion in 2004, up from $3.5 billion the previous year, an extraordinary 28% growth from 2003 to 2004. Additional findings based on IDC's research are summarized below:

- ☒ The motivation of hackers and the sophistication of threats have dramatically changed. Financial gain is the number 1 driving force behind the global spam epidemic, the outbreak of "phishing" scams, and the explosive growth of spyware.
- ☒ Spyware continues to move up the priority list of corporate security concerns. Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey.* IDC believes more than three-quarters of all corporate machines are infected with various forms of spyware.
- ☒ Spam continues to clog networks, servers, and inboxes with unwanted and often offensive content. The convenience and efficiency of email have been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial email. IDC believes the number of spam messages sent daily will almost double over the next few years, increasing from 23 billion in 2004 to 42 billion in 2008 (see *Worldwide Email Usage 2004–2008 Forecast: Spam Today, Other Content Tomorrow,* IDC #31782, August 2004).
- ☒ Email pipelines continue to be a favorite target for malicious attacks, including worms, viruses, hackers, and blended threats. Moreover, recent incidents have achieved widespread propagation at rates significantly faster than before. The use of spamming techniques to distribute malicious emails and viruses has also increased the speed with which these attacks can cause significant damage. As a result, propagation times for malicious email viruses have dropped from hours to minutes.
- ☒ There is a growing demand for solutions that protect against information leakage and violations of government and industry regulations. These solutions monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging (IM), peer to peer (P2P), file transfers, Web postings, and other types of messaging traffic.

Filing Information: September 2005, IDC #34023, Volume: 1, Tab: Vendors

TABLE OF CONTENTS

P

TABLE OF CONTENTS — Continued

LIST OF TABLES

P

LIST OF FIGURES

IN THIS STUDY

This study examines the secure content management market for the period 2002–2009, with vendor revenue trends and market growth forecasts. Worldwide market sizing is provided for 2004, with trends from 2003. A five-year growth forecast for this market is shown for 2005–2009. A vendor competitive analysis, with vendor revenues and market shares of the leading vendors, is provided for 2004. This study also includes profiles of leading vendors and identifies the characteristics that vendors will need to be successful in the future. This document updates the forecast published in *Worldwide Secure Content Management 2005–2009 Forecast: The Emergence of Outbound Content Compliance* (IDC #33076, March 2005).

Methodology

See the Learn More section for a description of the forecasting and analysis methodology employed in this study.

In addition, please note the following:

- The information contained in this study was derived from the IDC Software Market Forecaster database as of August 18, 2005.
- All numbers in this document may not be exact due to rounding.
- For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2005* (IDC #32884, February 2005).

Secure Content Management Market Definition

SCM includes policy-based content security solutions designed to secure, monitor, filter, and block threats from messaging and Web traffic. SCM protects against inbound threats such as spam, fraudulent emails, viruses, worms, trojans, spyware, and offensive material. SCM solutions are also designed to protect against outbound threats such as confidential data, customer records, intellectual property, and offensive content leaving an organization. SCM solutions play a key role in complying with government and industry regulations as well as enforcing corporate policies. SCM is a superset of three specific product areas:

- **Antivirus** software identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (e.g., instant messaging and short message service [SMS]) for any known or potential viruses, malicious code, trojans, or spyware.
- **Web filtering** software is used to screen and exclude from access or availability Web pages that are deemed objectionable or not business related. Web filtering is used by corporations to enforce corporate Internet use policies as well as by schools and universities and home computer owners (for parental controls).

- **Messaging security** software is used to monitor, filter, and/or block messages from different messaging applications (e.g., email, IM, SMS, and P2P) containing spam, company confidential information, and objectionable content. Messaging security is also used by certain industries to enforce compliance with privacy regulations (e.g., HIPAA, Gramm-Leach-Bliley [GLB], and SEC) by monitoring electronic messages for compliance violations. This market also includes secure (encrypted) email.

Executive Summary

SCM vendors enjoyed another strong year of growth in 2004. Major virus and worm outbreaks, continued increases in spam, corporate deadlines for compliance with government and industry regulations, and the explosive growth of spyware fueled the need for SCM security solutions. Viruses and worms continue to be the most serious threat facing corporations today, but spyware has rapidly climbed the priority list of enterprise security threats and now ranks as the second most serious threat facing corporations today.

Spyware has become both a security and system management nightmare. IDC believes more than three-quarters of all corporate machines are infected with various forms of spyware. Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number help desk calls related to spyware are forcing corporations of all sizes to take action.

Spam has climbed back up the priority list of IT managers and security departments and ranks as the third-greatest threat to enterprise security. Email phishing attacks are now daily occurrences for any organization, and especially for the largest financial institutions and their customers. The pure volume of spam continues to increase at a rapid pace. Spam clogs networks, servers, and inboxes with unwanted and often offensive content. The convenience and efficiency of email have been dramatically reduced by the extremely rapid growth in the volume of unsolicited commercial email. An increasing amount of spam is being sent by a botnet of zombie machines. In fact, IDC believes the majority of spam sent today originates from zombie machines remotely controlled by spammers.

An emerging threat to corporate security comes from inside the organization. The "insider threat" of trusted employees deliberately or inadvertently distributing sensitive information is quickly becoming a major concern in many organizations. The growing awareness of Outbound content compliance (OCC) was recently catalyzed by a series of corporate scandals in which customer records, confidential information, and intellectual property were leaked. As the vast majority of those cases demonstrate, such breaches are often not the result of malicious wrongdoing but rather employees who unknowingly put their companies at risk.

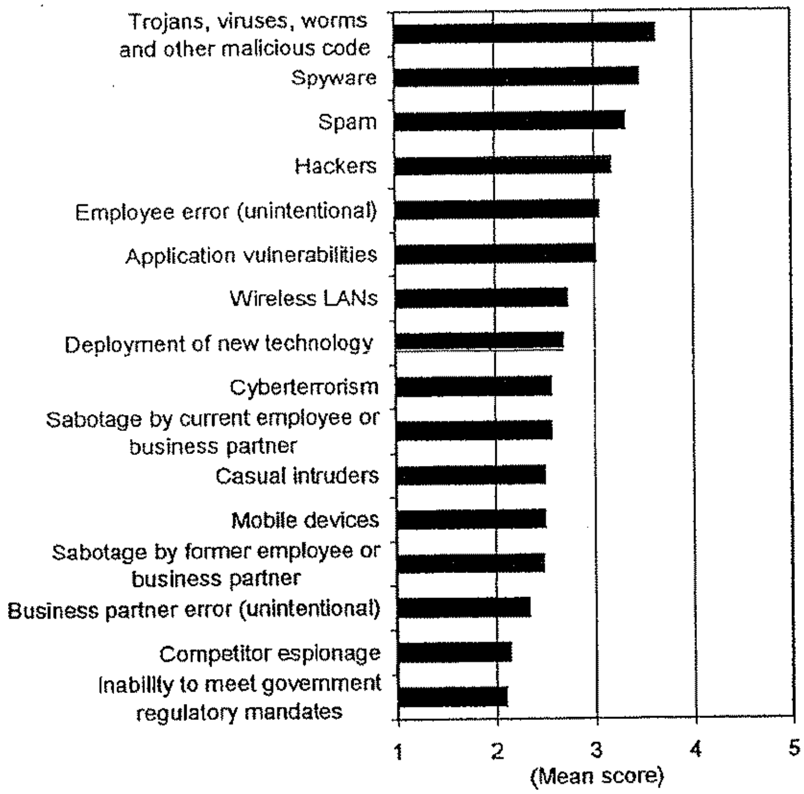
SITUATION OVERVIEW

Hot Trends in the Secure Content Management Market

Viruses and worms continue to be the most serious threat facing corporations today, but spyware has rapidly climbed the priority list of enterprise security threats and now ranks as the second most serious threat facing corporations today (as shown in Figure 1).

FIGURE 1

Threats to Enterprise Security



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's *Enterprise Security Survey*, 2005

Spyware: Motivated by Financial Gain

Spyware is now considered to be the second-greatest threat to enterprise network security, according to IDC's 2005 *Enterprise Security Survey,* up from fourth in 2004. Spyware has quickly become both a security and system management nightmare. IDC believes more than three-quarters of all corporate machines are infected with various forms of spyware. Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number help desk calls related to spyware are forcing corporations of all sizes to take action Our survey results indicate that 84% of organizations have implemented antispyware

Although the consequences of spyware may be as minor as annoying advertising pop-ups, spyware has the potential to do significant damage to the machine and also to the entire network. It has the ability to capture virtually all online activity. From monitoring all keystrokes, email snooping, and scanning files on the hard drive to changing system or registry settings, spyware is both a privacy and enterprise security threat. Such activities can lead to identity theft, data corruption, and, increasingly, theft of company trade secrets. Hackers are also using keyloggers to steal users' account information, log-in names, and passwords. With a user's account information, the hacker is then able to obtain a wealth of personal data, including bank information, additional passwords, and credit card numbers.

Spyware is far more sophisticated than traditional viruses, and the motivation of a spyware writer is drastically different from that of a virus writer. Spyware is not being created by the younger generation of script kiddies who create viruses, seeking personal pride or notoriety. Spyware writers, unlike virus writers, are motivated by profit and financial gain. The evolution from mischievous hobby to a money-making criminal venture has attracted a new breed of sophisticated hackers and organized crime. Hackers are now much less concerned with destroying systems and knocking out Web sites. They realize that they can generate money from stealing confidential personal information and corporate data and selling it to spammers or those involved in organized crime and fraud. IDC believes this profit-driven motivation will cause the number of attacks to increase in sophistication, frequency, and severity.

Spam: Threat on the Rise Again

Spam has once again climbed back up the priority list of IT managers. Spam moved from a nuisance in 2002 to a full-blown IT nightmare in 2003. As many organizations implemented antispam technologies during 2003 and 2004, spam started to slide back down the priority list in many IT departments. In fact, in IDC's 2004 *Enterprise Security Survey,* spam fell to eighth place on the list of most serious threats to enterprise security. This decline was quickly reversed, and spam is once again considered a major security threat, ranking as the third-greatest threat to enterprise security in 2005.

IDC believes there are several factors driving the threat resurgence of spam.

- Email phishing attacks are now daily occurrences for any organization, and especially for the largest financial institutions and their customers. The recent surge in email phishing attacks has created a sense of urgency within financial institutions, large Internet service providers (ISPs), security technology providers, law enforcement agencies, and even university research labs. These organizations are now working together to agree on technology solutions and best practices for curbing phishing attacks Until email authentication standards and new antiphishing solutions are widely adopted, however, phishing will continue to be a popular identity theft tactic. Financial Insights, an IDC company, estimates that global financial institutions lost $400 million or more in 2004 due to phishing schemes. IDC believes that more sophisticated attackers, often from organized crime, will increasingly use phishing techniques to obtain personal information to perpetrate identity theft. The number of phishing scams is rocketing, and IDC believes the sophistication and scale of online frauds and identity thefts will continue to increase at a rapid pace. Antispam technologies are playing a key role in the detection of phishing through URL and/or email content filtering.

- The pure volume of spam continues to increase at a rapid pace. Spam continues to clog networks, servers, and inboxes with unwanted and often offensive content. The convenience and efficiency of email have been dramatically reduced by the extremely rapid increase in the volume of unsolicited commercial email. IDC believes the number of spam messages sent daily will almost double over the next few years, increasing from 23 billion in 2004 to 42 billion in 2008 (see *Worldwide Email Usage 2004–2008 Forecast: Spam Today, Other Content Tomorrow*, IDC #31782, August 2004). The rising torrents of spam are reducing email's usefulness by forcing users and IT staff to expend additional time and energy to identify and delete spam and prevent spam from causing harm in the form of viruses, worms, and offensive content. ISPs and antispam solution vendors reported that spam currently represents 45–80% of all inbound Internet email, way up from 2002 levels closer to 15–30%.

- An increasing amount of spam is being sent by a bot network of zombie machines. In fact, IDC believes that the majority of spam sent today originates from zombie machines remotely controlled by spammers. The main challenge with stopping spam from bot networks is that the spam originates from thousands of different networks, and traditional DNS blacklists used by some antispam programs offer little protection. High-profile worms such as Sobig, MyDoom, and Bagle all contained malicious code that allowed remote attackers to take over infected machines. IDC believes zombie machines will continue to grow as the preferred distribution tool for spammers. Moreover, we believe zombie machines will increasing be used to send phishing scams, spread viruses, download pornography, and steal personal information.

- The use of spamming techniques to distribute malicious emails and viruses has also increased the speed with which these attacks can cause significant damage. As a result, propagation times for malicious email viruses have dropped from hours to minutes.

Outbound Content Compliance: Information Leakage and Data Protection

Historically, information security solutions have focused on addressing external threats to corporate networks and endpoints. Viruses, hackers, worms, trojans, spam, blended threats, and, most recently, spyware have wreaked havoc on corporate networks and users alike. In turn, enterprises have deployed an expanding array of security solutions such as firewall, antivirus, antispam, intrusion detection/prevention, and antispyware to protect the corporate perimeter from inbound threats. Today, an emerging threat to corporate security comes from inside the organization. The insider threat of trusted employees deliberately or inadvertently distributing sensitive information is quickly becoming a major concern in many organizations. This concern has created a new market, which IDC has termed outbound content compliance.

OCC includes solutions that monitor, secure/encrypt, filter, and block outbound content contained in email, instant messaging, P2P, file transfers, Web postings, and other types of messaging traffic. OCC solutions play a key role in enforcing corporate governance, which is defined by IDC as a combination of complying with both external regulatory requirements and internal corporate policies and best practices. These solutions help organization protect against the following:

☑ Violations of government and industry regulations (HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, and so on)

☑ Violations of corporate email policy and best practices

☑ Loss/leakage of intellectual property

☑ Loss/leakage of confidential or customer information

☑ Inappropriate content

The growing awareness of outbound content compliance was recently catalyzed by a series of corporate scandals in which customer records, confidential information, and intellectual property were leaked. As the vast majority of those cases demonstrate, such breaches are often not the result of malicious wrongdoing but rather employees who unknowingly put their companies at risk. This may occur as employees send out email messages that contain files or content they are not aware is confidential. Another example is employees delivering confidential files to their Web-based emailboxes, or copying files to mobile devices, and thus exposing them to untrusted environments. IDC believes enterprise rights management (ERM) solutions will also play a key role in preventing data leakage.

Enterprise Rights Management Gains Traction

The demand for solutions that safeguard confidential and sensitive data has been fueled by recent high-profile data thefts and government regulations. Security officers, compliance officers, and IT departments alike are all struggling to control the dissemination of and access to sensitive data contained in email, Word documents, and other types electronic document formats. An emerging set of solutions that IDC is defining as enterprise rights management is being deployed to address a broad spectrum of customer needs, including:

☑ Controlling access to and usage of confidential and sensitive information

☑ Preventing confidential and sensitive information from leaving an organization

☑ Protecting documents outside of the corporate firewall

☑ Ensuring compliance with government and industry regulatory requirements such as Gramm-Leach-Bliley, HIPAA, Sarbanes-Oxley, and SB 1386

☑ Enforcing policies around content creation, editing, sharing, publishing, and distribution

ERM has emerged from the digital rights management (DRM) market over the last decade in parallel with the proliferation of the Internet. Initially, it was aimed at providing publishing and media companies with new capabilities to control the use of digital content such as songs (MP3s), movies, electronic magazines, and so on. But the burst of the Internet bubble forced many DRM vendors out of the game, and others refocused by trying to address the corporate market.

ERM is aimed at providing encryption-based solutions for enforcing corporate digital content use and access policies throughout the information life cycle, covering content creation, editing, sharing, publishing and content distribution. Although these characteristics make ERM quite similar to "classic" media DRM at its essence, ERM is different in terms of some key issues. The most important one is the ability to centrally define and manage usage policies according to corporate requirements, taking it from the content author's hands. In addition, ERM products are usually designed to provide an audit trail of user activities, which is less necessary in media DRM (and may be seen as violating users' privacy). Key players in the enterprise rights management market include Microsoft, Workshare, Authentica, Adobe, Liquid Machines, SealedMedia, and other emerging vendors.

Microsoft Continues to Expand Its Security Arsenal

Microsoft's recent acquisitions of FrontBridge and Sybari are clear indications of a move into the enterprise security market. With FrontBridge and Sybari, Microsoft hopes to address the customer complaints that Microsoft Exchange environments are still suffering from too many malicious attacks, spam, system failures, and other messaging-related headaches. The acquisitions offer Microsoft customers a choice between a hosted service with FrontBridge or an onsite antivirus and antispam software with Sybari. The FrontBridge acquisition also gives Microsoft a set of services with which to enforce compliance through archiving of email in addition to blocking spam and viruses. Moreover, IDC believes this move helps Microsoft expand its Exchange-related revenue from one-time product sales and software maintenance fees to include an annuity-based revenue stream for security-related services that customers can easily deploy to central and remote sites.

The recent moves by Microsoft follow its acquisition of antivirus vendor GeCad in 2003 and antispyware vendor Giant Software in 2004. IDC believes GeCad and Giant will serve as not only the foundation of Microsoft's consumer OneCare security service, but also the foundation for an enterprise client security solution in the near future. We fully expect Microsoft to compete directly with established security vendors Symantec, McAfee, Trend Micro, Computer Associates (CA), and Sophos for both enterprise and consumers deals. In addition to the acquisitions, Microsoft signed a nonexclusive worldwide agreement with Finjan to license patents for computer security technologies. Finjan is a leading provider of behavior-based secure content management solutions that complement signature-based antivirus and intrusion detection solutions.

On the consumer side, Microsoft announced plans to deliver Windows OneCare, a consumer subscription service that will provide automated protection, maintenance, and performance tuning as an all-in-one package for Windows-based PCs. Although Microsoft claims to be targeting the 70% of consumer PC users who don't have antivirus protection, IDC believes OneCare will also compete for the current consumer installed base of Symantec and McAfee. We believe that the OneCare subscription service to consumers will be priced competitively, but slightly lower than current antivirus subscription rates. In the longer term (24–48 months), we expect that pricing for consumer security solutions will gradually fall as Microsoft begins to take share from the leading antivirus vendors. We do not believe, though, that price deflation will cause overall consumer security spending to decline — the increasing number of subscribers will offset the price deflation. We also believe that Microsoft will target the small office and home office segments for OneCare subscriptions.

Web Filtering: No Longer Just a Productivity Tool

Web filtering has evolved from addressing a single class of employee distractions — access to inappropriate URLs — to more comprehensive Web security solutions that address a wide array of Web-based threats. Web security concerns are at an all-time high due to the rash of spyware, virus, phishing, and malicious mobile code attacks that have wreaked havoc on corporate networks. The number of Web sites distributing spyware has increased explosively as spyware creators continue to extend their distribution channels. As the number of Internet users continues to increase, the Web becomes an increasingly more attractive target for hackers, spyware, and virus writers. Moreover, attacks targeting Web browser vulnerabilities illustrate the sophisticated techniques hackers have developed to spoof, or fake, Web sites and how easily malicious code can steal usernames, passwords, and other vital information. IDC believes Web-based attacks will continue to become more malicious and sophisticated. Web filtering solutions will play a valuable role as a complementary enhancement to traditional antivirus and firewall deployments.

Performance of Leading Vendors in 2004

Table 1 displays 2003–2004 worldwide revenue and 2004 growth and market share for secure content management vendors. Worldwide revenue for the SCM market reached $4.5 billion in 2004, representing a 27.8% increase over 2003. Vendor market shares for software, appliance, and hosted service-based SCM solutions are shown graphically in Figures 2–4.

TABLE 1

Worldwide Secure Content Management Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Symantec Corp.	1,138.9	1,440.2	26.5	32.2
McAfee Inc.	597.6	620.8	3.9	13.9
Trend Micro	403.6	547.6	35.7	12.2
Sophos	105.0	129.4	23.3	2.9
Websense	81.7	111.9	37.0	2.5
Panda Software	65.0	104.0	60.0	2.3
Computer Associates International Inc.	76.9	103.0	33.9	2.3
SurfControl Inc.	79.7	93.6	17.5	2.1
Sybari Software Inc.	44.2	54.4	23.1	1.2
F-Secure Corp.	37.8	51.3	35.7	1.1
CipherTrust	26.0	50.2	93.1	1.1
Clearswift Corp.	36.3	44.9	23.7	1.0
MessageLabs	35.6	43.9	23.4	1.0
Tumbleweed Communications Corp.	31.8	41.0	29.0	0.9
Secure Computing Corp.	31.1	33.0	6.1	0.7
Norman ASA	24.3	31.5	29.6	0.7
Postini	24.9	30.7	23.2	0.7
Ahnlab Inc.	21.9	28.3	29.3	0.6
Webroot	8.5	23.5	176.5	0.5
Kaspersky Lab	13.9	22.9	64.7	0.5
Aladdin Knowledge Systems	12.7	21.5	69.3	0.5

TABLE 1

Worldwide Secure Content Management Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Entrust Inc.	18.0	21.0	16.7	0.5
IronPort	8.0	20.6	157.5	0.5
Sendmail	11.3	18.6	64.6	0.4
FrontBridge	7.5	18.5	146.7	0.4
Webwasher	12.5	15.4	23.4	0.3
GROUP Technologies	12.2	15.0	23.4	0.3
SonicWALL	10.1	14.0	38.6	0.3
Finjan Software Ltd.	9.3	12.9	38.7	0.3
ZixCorp	10.5	12.9	22.9	0.3
Vericept	7.8	12.0	53.8	0.3
MiraPoint	5.5	11.3	105.5	0.3
Cloudmark	7.5	10.5	40.0	0.2
St. Bernard Software	7.8	10.0	28.2	0.2
BorderWare	4.0	9.0	125.0	0.2
Barracuda Networks	2.1	8.9	323.8	0.2
8e6 Technologies	8.1	8.8	8.6	0.2
Proofpoint	3.0	8.7	190.0	0.2
Hauri Inc.	6.5	8.5	29.8	0.2
FaceTime*	5.5	8.0	45.5	0.2
IMlogic*	3.9	8.0	105.1	0.2
Aluria Software	2.5	7.5	200.0	0.2
NetIQ	10.0	7.3	-26.7	0.2
Sigaba	5.5	6.8	23.0	0.2
Tenebril	2.2	6.5	195.5	0.1

TABLE 1

Worldwide Secure Content Management Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Blue Coat	2.5	6.3	152.0	0.1
MailFrontier	2.6	6.2	138.5	0.1
Telemate	4.5	6.0	33.3	0.1
MX Logic	1.7	5.9	247.1	0.1
Tablus	1.5	5.0	233.3	0.1
eSoft	3.0	4.5	50.0	0.1
Akonix	2.1	3.6	71.4	0.1
Mail-Filters	1.3	3.5	169.2	0.1
Subtotal	3,097.7	3,949.3	27.5	88.2
Other	407.7	530.1	30.0	11.8
Total	3,505.4	4,479.4	27.8	100.0

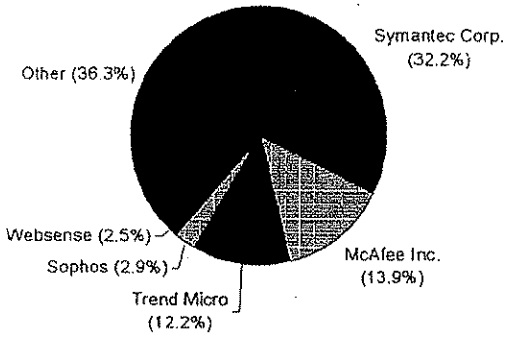
* Because of the private nature of these two companies and the wide range of revenue input available from multiple sources, we believe that these estimates have a 15–20% margin of error that precludes us from determining which of the two generated more revenue in 2004

Note: Vendor revenue includes hosted service–, software-, and appliance-based solutions.

Source: IDC, 2005

FIGURE 2

Worldwide Secure Content Management Software Revenue Share by Top 5 Vendor, 2004

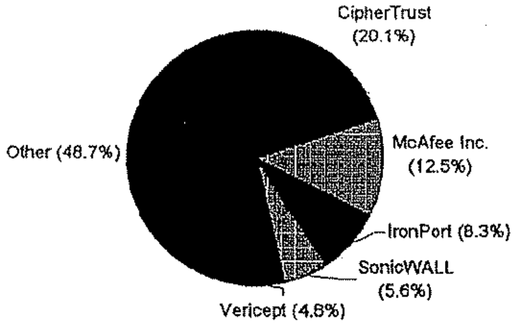


Total = $4.48B

Source: IDC, 2005

FIGURE 3

Worldwide Secure Content Management Appliance Revenue Share by Top 5 Vendor, 2004

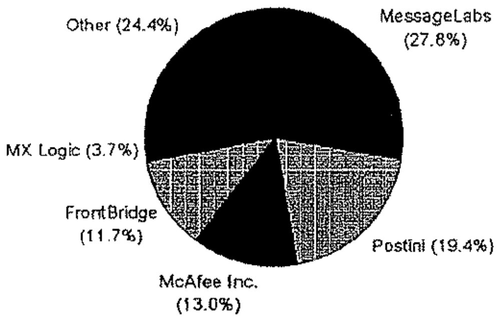


Total = $249.2M

Source: IDC, 2005

FIGURE 4

Worldwide Secure Content Management Hosted Service Revenue Share by Top 5 Vendor, 2004



Total = $158.0M

Note: McAfee revenue includes only McAfee ASaP business.

Source: IDC, 2005

Vendor Performance by Market Segment

Antivirus

Antivirus accounted for the largest segment of the SCM market in 2004, reaching $3.3 billion. From 2003 to 2004, the antivirus software market increased 22.3%.

Table 2 displays 2003–2004 worldwide revenue and 2004 growth and market share for antivirus vendors.

Messaging Security

Messaging security accounted for the second-largest segment of the SCM market in 2004, reaching $665.4 million. From 2003 to 2004, the messaging security software market increased 50.4%.

Table 3 displays 2003–2004 worldwide revenue and 2004 growth and market share for messaging security software vendors.

Web Filtering

Web filtering accounted for the third-largest segment of the SCM market in 2004, reaching $433.5 million. From 2003 to 2004, the Web filtering market increased 22.9%.

Table 4 displays 2003–2004 worldwide revenue and 2004 growth and market share for Web filtering software vendors. Vendor market shares for software and appliances are shown in Figures 5 and 6, respectively.

Antispyware

Antispyware accounted for the smallest, but fastest-growing, segment of the SCM market in 2004, reaching $97 million. From 2003 to 2004, the antispyware market increased 240.4%

Table 5 displays 2003–2004 worldwide revenue and 2004 growth and market share for antispyware vendors.

TABLE 2

Worldwide Antivirus Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Symantec Corp.	1,098.0	1,363.9	24.2	41.5
McAfee Inc.	577.5	597.2	3.4	18.2
Trend Micro	382.5	517.8	35.4	15.8
Sophos	96.6	116.5	20.6	3.5
Panda Software	65.0	104.0	60.0	3.2
Computer Associates International Inc.	61.5	74.2	20.6	2.3
F-Secure Corp.	35.9	51.3	42.9	1.6
Sybari Software Inc.	30.6	43.5	42.1	1.3
Norman ASA	23.1	31.5	36.4	1.0
Ahnlab Inc.	20.8	28.3	36.1	0.9
MessageLabs	19.8	26.4	33.1	0.8
Kaspersky Lab	13.9	22.9	64.7	0.7
Aladdin Knowledge Systems	10.0	16.8	68.0	0.5
Hauri Inc.	6.5	8.5	30.1	0.3
Finjan Software Ltd.	6.1	7.3	19.7	0.2
SonicWALL	4.2	6.4	60.0	0.2

TABLE 2

Worldwide Antivirus Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Blue Coat	2.0	5.3	165.0	0.2
Sendmail	1.3	2.6	100.0	0.1
Subtotal	2,447.8	3,009.9	23.0	91.7
Other	237.7	273.6	15.1	8.3
Total	2,685.6	3,283.5	22.3	100.0

Note Vendor revenue includes hosted service–, software-, and appliance-based solutions.

Source: IDC, 2005

TABLE 3

Worldwide Messaging Security Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Symantec Corp.	49.3	61.9	25.7	9.3
CipherTrust	26.0	50.2	93.1	7.5
Tumbleweed Communications Corp.	31.8	41.0	29.0	6.2
Clearswift Corp.	32.7	40.9	25.1	6.1
Postini	18.3	27.6	50.6	4.1
SurfControl Inc.	17.4	25.3	45.3	3.8
Trend Micro	16.1	23.4	45.3	3.5
Entrust Inc.	18.0	21.0	16.7	3.2
IronPort	8.0	20.6	157.5	3.1
FrontBridge	7.5	18.5	146.7	2.8
McAfee Inc.	11.5	17.7	54.7	2.7
MessageLabs	13.2	17.6	33.1	2.6
Sendmail	10.0	16.0	60.0	2.4

TABLE 3

Worldwide Messaging Security Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
GROUP Technologies	12.2	15.0	23.4	2.3
Sophos	8.4	12.9	54.1	1.9
Vericept	7.8	12.0	53.8	1.8
MiraPoint	5.5	11.3	105.5	1.7
Sybari Software Inc.	7.7	10.9	42.1	1.6
Cloudmark	7.5	10.5	40.0	1.6
Barracuda Networks	2.1	10.0	376.2	1.5
BorderWare	4.0	9.0	125.0	1.4
FaceTime*	5.5	8.0	45.5	1.2
IMlogic*	3.9	8.0	105.1	1.2
Sigaba	5.5	6.8	23.0	1.0
Proofpoint	3.0	6.5	116.7	1.0
ZixCorp	4.7	6.5	36.9	1.0
MailFrontier	2.6	6.2	138.5	0.9
MX Logic	1.7	5.9	247.1	0.9
NetIQ	7.0	5.9	-16.2	0.9
Tablus	1.5	5.0	233.3	0.8
Blue Coat (Proxy AV)	2.5	5.0	100.0	0.8
Aladdin Knowledge Systems	2.7	4.7	74.1	0.7
Esoft	3.0	4.5	50.0	0.7
Akonix	2.1	3.6	71.4	0.5
Mail-Filters	1.3	3.5	169.2	0.5
Computer Associates International Inc.	1.8	2.1	12.6	0.3
Webwasher	1.1	1.5	40.2	0.2

TABLE 3

Worldwide Messaging Security Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Finjan Software Ltd.	1.0	1.2	20.0	0.2
St. Bernard Software	0.1	0.5	400.0	0.1
Subtotal	365.9	558.6	52.7	84.0
Other	76.6	106.8	39.4	16.0
Total	442.5	665.4	50.4	100.0

* Because of the private nature of these two companies and the wide range of revenue input available from multiple sources, we believe that these estimates have a 15–20% margin of error that precludes us from determining which of the two generated more revenue in 2004

Note· Vendor revenue includes hosted service–, software-, and appliance-based solutions.

Source: IDC, 2005

TABLE 4

Worldwide Web Filtering Product Revenue by Vendor, 2003 and 2004 ($M)

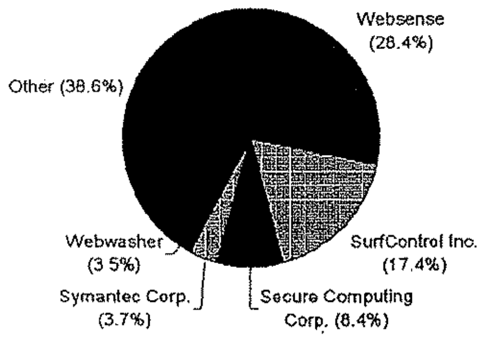
	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Websense	81.7	111.9	37.0	25.8
SurfControl Inc.	62.4	68.3	9.5	15.8
Secure Computing Corp.	31.1	33.0	6.1	7.6
Symantec Corp.	11.6	14.4	23.9	3.3
Webwasher	9.6	13.9	44.1	3.2
St. Bernard Software	7.7	9.5	23.4	2.2
8e6 Technologies	8.1	8.5	4.9	2.0
SonicWALL	5.9	7.6	28.8	1.8
ZixCorp	5.8	6.5	11.2	1.5
Trend Micro	5.0	6.4	28.0	1.5
Telemate	4.5	6.0	33.3	1.4
Clearswift Corp.	3.6	4.0	11.4	0.9
NetIQ	3.0	1.5	-51.1	0.3
Finjan Software Ltd.	1.0	1.3	30.0	0.3
Computer Associates International Inc.	0.6	1.0	68.9	0.2
Subtotal	241.7	293.8	21.6	67.8
Other	111.2	139.7	25.7	32.2
Total	352.8	433.5	22.9	100.0

Note: Vendor revenue includes hosted service--, software-, and appliance-based solutions.

Source: IDC, 2005

FIGURE 5

Worldwide Web Filtering Software Revenue Share by Top 5 Vendor, 2004

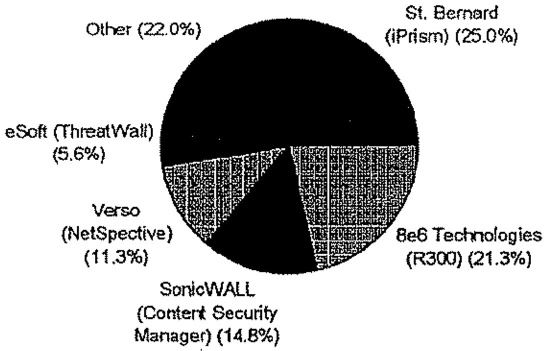


Total = $393.5M

Source: IDC, 2005

FIGURE 6

Worldwide Web Filtering Appliance Revenue by Top 5 Vendor, 2004



Total = $40.0M

Source: IDC, 2005

TABLE 5

Worldwide Antispyware Product Revenue by Vendor, 2003 and 2004 ($M)

	2003	2004	2003–2004 Growth (%)	2004 Share (%)
Computer Associates International Inc.	7 5	25 8	243 3	26.5
Webroot	6.5	23.5	261.5	24.2
Aluria Software	2 5	7 5	200 0	7.7
Tenebril	2.2	6.5	195.5	6.7
InterMute (acquired by Trend Micro)	2.0	4.0	100.0	4.1
Finjan Software Ltd.	1.2	3.1	158.3	3.2
Subtotal	21.9	70.4	221.2	72.5
Other	6.6	26.7	303.8	27.5
Total	28.5	97.0	240.4	100.0

Note. Vendor revenue includes hosted service–, software-, and appliance-based solutions.

Source: IDC, 2005

FUTURE OUTLOOK

Forecast and Assumptions

Worldwide

IDC's estimate of the growth of the secure content management market through 2009 is presented in Table 6. Worldwide revenue for the SCM software market is forecast to increase from $4.5 billion in 2004 to $10.5 billion in 2009, representing an 18.7% compound annual growth rate (CAGR). The forecast is broken out as follows:

- Antivirus will increase from $3.3 billion in 2004 to $6.4 billion in 2009, representing a 14.2% CAGR.
- Messaging security will increase from $665 million in 2004 to $2.6 billion in 2009, representing a 31.3% CAGR.
- Web filtering will increase from $433 million in 2004 to $929 million in 2009, representing a 16.5% CAGR.
- Antispyware will increase from $97 million in 2004 to $641 million in 2009, representing a 45.9% CAGR.

TABLE 6

Worldwide Secure Content Management Product Revenue by Segment, 2003–2009 ($M)

	2003	2004	2005	2006	2007	2008	2009	2004 Share (%)	2004–2009 CAGR (%)	2009 Share (%)
Antivirus	2,685.6	3,283.5	3,874.5	4,455.7	5,079.5	5,714.4	6,366.2	73.3	14.2	60.4
Antispyware	28.5	97.0	214.8	353.1	481.6	565.1	641.4	2.2	45.9	6.1
Web filtering	352.8	433.5	521.4	622.1	724.0	829.5	929.0	9.7	16.5	8.8
Messaging security	442.5	665.4	913.7	1,237.4	1,634.9	2,098.4	2,597.5	14.9	31.3	24.7
Total	3,509.4	4,479.4	5,524.4	6,668.2	7,920.0	9,207.5	10,534.1	100.0	18.7	100.0

Notes:

Vendor revenue includes hosted service–, software-, and appliance-based solutions.

See Table 10 for key forecast assumptions.

Source: IDC, 2005

By Platform

The worldwide SCM forecast by platform is shown in Table 7. SCM software will remain the largest segment throughout the forecast, but SCM appliances will be the fastest-growing segment (47% CAGR), followed by SCM hosted services (36% CAGR).

By Geographic Region

IDC analysts around the globe supplied regional input and insight into the SCM market forecast. The worldwide forecast is the aggregation of this regional data as reported in Table 8.

TABLE 7

Worldwide Secure Content Management Product Revenue by Platform, 2003–2009 ($M)

	2003	2004	2005	2006	2007	2008	2009	2004 Share (%)	2004–2009 CAGR (%)	2009 Share (%)
Software	3,288.5	4,072.2	4,844.9	5,621.3	6,454.8	7,273.9	8,069.2	90.9	14.7	76.6
Appliance	130.8	249.2	425.4	680.2	990.0	1,335.1	1,727.6	5.6	47.3	16.4
Hosted service	86.1	158.0	254.1	366.8	475.2	598.5	737.4	3.5	36.1	7.0
Total	3,505.4	4,479.4	5,524.4	6,668.2	7,920.0	9,207.5	10,534.1	100.0	18.7	100.0

Notes:

McAfee hosted services revenue includes only the McAfee ASaP offering. It does not include the McAfee.com consumer online subscription revenue.

See Table 10 for key forecast assumptions.

Source: IDC, 2005

TABLE 8

Worldwide Secure Content Management Product Revenue by Region, 2003–2009 ($M)

	2003	2004	2005	2006	2007	2008	2009	2004 Share (%)	2004–2009 CAGR (%)	2009 Share (%)
North America	1,597.0	1,984.0	2,423.4	2,899.5	3,403.3	3,900.2	4,387.3	44.3	17.2	41.6
Western Europe	1,167.0	1,534.0	1,889.4	2,279.7	2,698.9	3,120.3	3,541.9	34.2	18.2	33.6
Asia/ Pacific	574.4	754.0	956.0	1,178.7	1,446.1	1,746.3	2,086.8	16.8	22.6	19.8
ROW	167.0	207.3	255.7	310.4	371.7	440.6	518.2	4.6	20.1	4.9
Worldwide	3,505.4	4,479.4	5,524.4	6,668.2	7,920.0	9,207.5	10,534.1	100.0	18.7	100.0

Note: See Table 10 for key forecast assumptions.

Source: IDC, 2005

By Operating Environment

This study represents IDC's operating environment forecast for the SCM market through 2009. The revenue forecast for the SCM market, segmented by operating environment, is shown in Table 9.

TABLE 9

Worldwide Secure Content Management Product Revenue by Operating Environment, 2003–2009 ($M)

	2003	2004	2005	2006	2007	2008	2009	2004 Share (%)	2004–2009 CAGR (%)	2009 Share (%)
Mainframe	5.4	8.5	8.8	8.9	9.0	8.9	8.6	0.2	0.2	0.1
OS/400	2.9	3.9	4.0	4.1	4.1	4.1	4.0	0.1	0.5	0.0
Unix	418.9	542.9	608.6	673.8	742.2	809.4	862.3	12.1	9.7	8.2
Linux/other open source	119.3	152.7	252.4	397.6	598.8	858.4	1,211.7	3.4	51.3	11.5
Other multiuser	92.2	114.9	116.1	115.8	115.0	113.0	108.1	2.6	-1.2	1.0
Windows 32 and 64	2,765.8	3,524.7	4,375.5	5,280.3	6,233.0	7,163.6	8,057.4	78.7	18.0	76.5
Embedded	12.1	15.7	20.2	26.0	33.5	43.2	54.5	0.3	28.3	0.5
Other single user	85.7	111.9	133.3	154.3	174.5	193.7	210.2	2.5	13.4	2.0
Platform independent	3.0	4.2	5.6	7.4	9.9	13.2	17.3	0.1	32.7	0.2
Total	3,505.4	4,479.4	5,524.4	6,668.2	7,920.0	9,207.5	10,534.1	100.0	18.7	100.0

Note: See Table 10 for key forecast assumptions.

Source: IDC, 2005

Key Forecast Assumptions

Table 10 lists the key assumptions used to generate the forecast.

TABLE 10

Key Forecast Assumptions for the Worldwide Secure Content Management Market, 2005–2009

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Macroeconomics				
Economy	Worldwide economic growth will peak in 2005 and remain positive for at least three more years as the recovery runs it course.	**High.** The economy is now a positive influence on IT spending.	↑	★★★★☆
Unemployment/job creation	Unemployment worldwide will slowly drop, with the U.S. rate dropping under 5% by the end of 2005. Unemployment (and job creation) will be a much-watched indicator, with monthly results mixed.	**High.** More employment drives more need for IT infrastructure and is a lagging indicator of economic recovery; job creation should be accompanied by willingness to invest in other areas. Less unemployment means higher prices and more motivation to automate tasks through IT, long term.	↑	★★★★☆
Exchange rates	Long term, there will be declines in the dollar. Short term, uncertainty in the EU has caused the dollar to firm up. China will revalue and the dollar will slip further, but we expect this process to be gradual.	**Moderate.** A declining dollar makes U.S. IT products and software less expensive, but this will have a minor effect on regional growth because most U.S. companies sell via overseas subsidiaries and these use local currency. Still, results get reported in dollars, and this measure will look unrealistically better.	↑	★★★★☆
Stocks	In 2004, the stock market remained essentially flat. In 2005, we expect the stock market to stay flat with possible oscillations. Oil price fluctuations and international politics will play a significant role in market uneasiness.	**Moderate.** In spite of a rising economy, a fluctuating stock market increases riskiness.	↓	★★★☆☆

TABLE 10

Key Forecast Assumptions for the Worldwide Secure Content Management Market, 2005–2009

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Corporate profits	In 2005, profits will be lower than 15%, but still positive. Profit growth, though lower than in 2004, is expected to be positive, especially for the United States. Much of the early growth was from cost cutting, but more is now coming from added revenue.	**Moderate.** IT spending will continue to increase as companies look to the top line for increased profits.	↑	★★★★☆
Geopolitics	Terrorism alerts will remain high, and terrorism will increase with at least one major incident in the forecast period.	**Moderate.** New venues always increase uncertainty for a considerable period of time.	↓	★★★☆☆
Compliance	Attention to compliance will drive marginal new demand.	**Moderate.** Compliance regulations may begin to have an effect on software spending in 2005 and beyond.	↑	★★★★★
Technology/service developments				
Software complexity	Complexity will increase.	**High.** The complexity crisis will require new investment to cope.	↑	★★★★★
Linux	Open source will gain share.	**Low.** This change will have a downward impact on price pressures, but it will drive some new spending in proprietary software to manage and interoperate with Linux OSS.	↔	★★★★★
Mobility	Some compelling mobile applications will emerge in many industries.	**Moderate.** This will drive marginal new applications.	↑	★★★★☆
Killer apps	The next killer solution will involve two-factor biometrics led by successful Microsoft application demonstrations.	**Moderate.** This will be industry-by-industry combat against the doubters.	↑	★★★☆☆

TABLE 10

Key Forecast Assumptions for the Worldwide Secure Content Management Market, 2005–2009

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Labor supply				
Offshoring	Offshoring will increase.	**Low.** Offshoring will drive demand for low-cost (open source) exports from the United States and Europe long term.	↑	★★★☆☆
Productivity management	The search for productivity improvements will continue.	**Moderate.** This search will impact increasing software revenue growth in custom development and start-ups.	↑	★★★☆☆
Capitalization				
Venture	Venture funding will continue to increase slowly.	**Low.** Money will continue to open up.	↑	★★★☆☆
Stocks	The housing market will slow and inhibit consumer liquidity, causing a minor recession.	**High.** There will be an impact on consumer and prosumer markets and software in industries that supply them.	↓	★☆☆☆☆
Market characteristics				
Large enterprise software renewals	There will be extreme price pressure on large enterprise software renewals.	**Moderate.** This pressure will have an impact on software revenue growth. Some software brokers will figure out the new value proposition and will pull ahead of the overall market, but this will be about taking share away from the laggards.	↔	★★☆☆☆
Security	The market will remain populated by many, many vendors selling myriad products with many different marketing messages. There will be a lot of options in the market.	**Moderate.** The large number of vendors leads to innovation and market education, thus creating more demand, especially for advanced solutions such as SCM.	↑	★★★★☆

TABLE 10

Key Forecast Assumptions for the Worldwide Secure Content Management Market, 2005–2009

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Hardware	Security appliances will continue to grow in popularity as an easy way to distribute software security solutions to customers. They also have a limited life due to performance requirements and need to be periodically updated.	**High.** Appliances will continue to be popular with customers and distributors. There will be a replacement cycle associated with this market.	↑	★★★★☆
The Internet	Internet adoption is still going strong, especially in emerging economies. In the next three years, 300 million new users will come online and commerce will grow threefold. By the end of 2005, 40% of Internet households will be broadband.	**Moderate.** Analysts and pundits may underestimate the impact of the Internet because the "buzz" is gone. It will be enabler for both new markets and new business models. These emerging economies provide considerable opportunity for security appliances.	↑	★★★★☆
Consolidation	Smaller pure-play vendors will be open to mergers and acquisitions that enable them to reach wider audiences, while larger firms with broader product portfolios will look for technology and product acquisitions to fill gaps to be able to offer end-to-end solutions from a single source.	**Low.** Market consolidation, or lack thereof, will have a limited impact on the overall SCM markets.	↔	★★★★☆
Consumption				
Buying sentiment	IT buyers will continue to be inhibited by uncertainty.	**High.** These trends are already factored into our forecast.	↓	★★★★☆
Saturation	New markets will be found in emerging economies, and the large ones are India and China.	**High.** These trends are already factored into our forecast.	↑	★★★★☆

Legend: ★☆☆☆☆ very low, ★★☆☆☆ low, ★★★☆☆ moderate, ★★★★☆ high, ★★★★★ very high

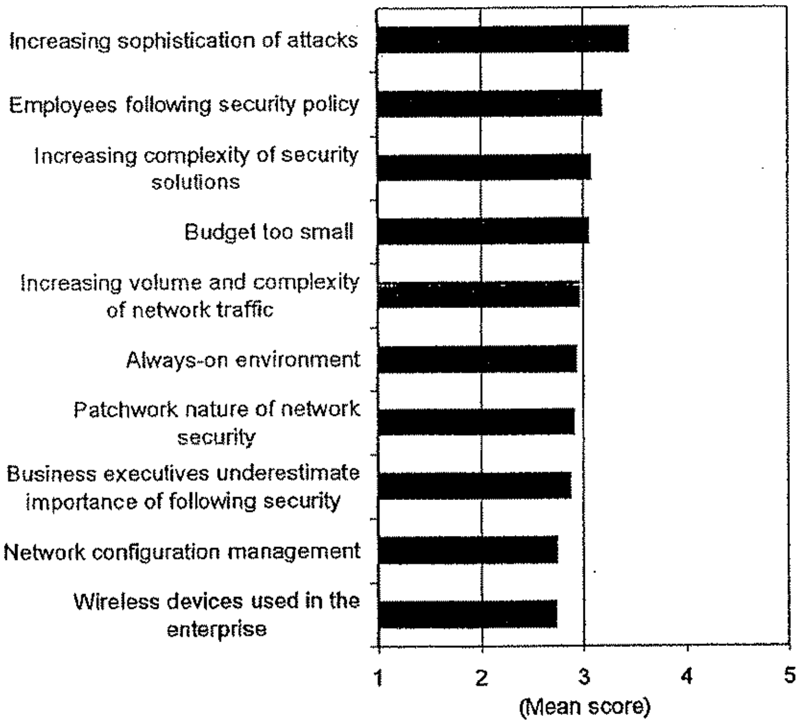
Source: IDC, 2005

ESSENTIAL GUIDANCE

IDC believes attacks on corporate networks, corporate PCs, and consumers will continue to increase in sophistication, frequency, and severity. Our survey results clearly show that the increasing sophistication of attacks is regarded as the top security challenge organizations face over the next 12 months (see Figure 7). We believe this will drive the demand for more proactive security products and services.

FIGURE 7

Security Challenges Organizations Face over the Next 12 Months



n = 435

Note: Scores are based on a scale from 1 to 5, with 1 being no challenge and 5 being a significant challenge.

Source: IDC, 2005

Our survey also revealed that the complexity of managing security technologies is another key challenge organizations will face over the next year. IDC believes this will continue to drive the need for more integrated solutions. SCM is increasingly moving away from a focus on a single type of protection, such as antivirus, toward a focus on broad protection from a wide range of emerging threats to enterprise security.

Employees following security policies is another key area of concern over the next 12 months. IDC believes this concern will have a direct impact on the OCC market discussed previously in this study. The insider threat of trusted employees deliberately or inadvertently distributing sensitive information is quickly becoming a major concern across all vertical industries. We expect to see more examples of corporate scandals in which customer records, confidential information, and intellectual property are leaked. This will fuel the demand for solutions that monitor, secure/encrypt, filter, and block sensitive information contained in email, instant messaging, P2P, file transfers, Web postings, and other types of messaging traffic.

Vendor Profiles

Symantec Corp.

Overview

Symantec is a United States–based company that was founded in 1982. The company held its initial public offering in June of 1989 and is headquartered in Cupertino, California. Employer to more than 14,000 people, Symantec has operations in more than 40 countries, including all over the United States as well as in Canada, New Zealand, Japan, and Australia. Symantec recently acquired Brightmail Inc., a global antispam market leader. Symantec now protects more than 1,800 enterprises globally and provides spam protection for the leading Internet service providers, including AT&T WorldNet, Cox Communications, EarthLink, MSN, TelstraClear, Xtra, and Verizon Online. Symantec protects approximately 300 million mailboxes worldwide. The acquisition of Brightmail positions Symantec as an industry leader in antispam solutions.

Within the last week, Symantec announced that it signed an agreement to acquire Sygate Technologies, an endpoint compliance solutions vendor. Sygate's technology will complement Symantec's presence on the endpoint to address the security, compliance, and remediation requirements of today's large enterprises.

Secure Content Management Products

Symantec offers the following SCM products:

- Symantec Antivirus and Norton Antivirus offer extensive virus protection and removal for both consumer and corporate environments. Symantec's corporate offering provides protection at the client, host, and Internet gateway levels of a corporate network. Its functionality extends to scan email attachments in both Domino and Exchange collaborative environments.

- Symantec's Norton Internet Security 2005 AntiSpyware Edition provides protection from viruses, hackers, and privacy threats. It includes Norton Spyware Protection, which automatically detects and removes both spyware and adware. The all-in-one protection of Norton Internet Security also helps prevent email fraud and keep confidential information safe.

- ☒ Symantec Mail-Gear resides on a corporate mail server and scans incoming and outgoing mail for inappropriate content. It provides comprehensive, policy-based email and attachment scanning and filtering to protect organizations against liability claims, spam attacks, and the loss of proprietary information. Symantec Brightmail Anti-Spam offers spam catching that prevents false positives. It provides spam protection that defends against real-time spam attacks, and also proactively identifies first-time spam.

- ☒ Symantec Premium Anti-Spam is an add-on subscription service that provides spam prevention for Symantec Mail Security and Symantec AntiVirus Enterprise Edition customers. Symantec's global Brightmail Logistics Operations Centers in the United States, Ireland, Australia, and Taiwan analyze spam where it occurs across the globe

Strategic Direction

On a revenue basis, Symantec is the worldwide leader in security software, a broad market that can include SCM, antivirus, antispam, intrusion detection/prevention systems, vulnerability assessment and management solutions, firewall/VPN solutions, and security 3A solutions (authentication, authorization, and administration). The firm enjoys long-standing OEM relationships with HP, IBM, Gateway, and Cisco (Linksys), which put its Norton line of products on more than 50 million new PCs and 4 million firewall and router products worldwide each year, crossing both business and consumer markets.

Symantec's $370 million acquisition of Brightmail, announced on May 19, 2004, underscores the market reality that customers prefer to buy comprehensive messaging security solutions rather than point (i.e., antispam or antivirus) products. The acquisition also allows Symantec to pair its strong position in both the consumer and business security markets with Brightmail's early-to-market reputation as a technology provider and OEM partner to ultimately expand Symantec's sales reach and product breadth. In addition, Symantec will look to leverage the huge volume of email traffic passing through the Brightmail filtering process as a new source of early warning on impending threats.

This acquisition of Brightmail and the pending acquisition of Sygate Technologies are further examples of the consolidation occurring in the Internet security market that will lead to antispam protection becoming a commodity and small antispam vendors looking to partner with large firms in the broader security space to be pulled into the big deals.

McAfee Inc.

Overview

Founded in 1989, McAfee held its initial public offering in 1992. The company is headquartered in Santa Clara, California, with approximately 3,900 people currently under its employ. McAfee has worldwide offices in more than 35 countries with major operations across the United States, in India, and in the United Kingdom. Formerly Network Associates, the company changed its name to McAfee on July 1, 2004.

Secure Content Management Products

McAfee offers the following SCM products:

- McAfee Antivirus offers virus protection/elimination for consumer and enterprise environments. It protects at the client, server, and gateway levels, integrating with email and file servers and even PDAs to detect and eliminate viruses. It also offers policy-based spam protection in Exchange, Domino, and WebShield environments.

- Managed VirusScan is an online enterprise antivirus service that provides continuously updated protection against viruses and malicious code. It provides continuous protection to the desktop against viruses and worms

- Managed VirusScreen is an online enterprise antivirus service that stops email-borne viruses and infected attachments before they enter the network. It screens streaming email and either cleans it or quarantines it before it reaches the mail server.

- McAfee AntiSpyware protects against unwanted programs such as spyware, adware, dialers, tracking cookies, and other unwelcome marketing programs. It monitors Internet security settings, detects changes to browser settings and system files, and updates automatically.

- McAfee Spam Killer offers an AntiPhishing Internet Explorer plug-in, which protects personal and financial information against known phishing scams by blocking access to known and potentially fraudulent identity theft Web sites.

- McAfee Security Shield for Microsoft ISA Server provides protection over Internet and mail content, including filtering rules that can be defined per user group, support for all major protocols, centralized policy management, and graphical reporting.

- McAfee.online consumer services protects consumer PCs, files, and email address books from all types of malware including viruses, worms, Trojans, spyware, spam, and phishing.

Strategic Direction

McAfee is committed to protecting the servers and networks of home users, small businesses, and large enterprises from existing and emerging threats and malicious code. The company provides best-of-breed intrusion prevention and risk management solutions that allow customers to block both known and unknown attacks.

On June 2, 2005, McAfee acquired Wireless Security Corp., a privately held company that offers WiFi security solutions for home and small business wireless networks to prevent unauthorized access to a wireless network, its contents, or Internet service. The bundling of McAfee's security solutions, McAfee Internet Security Suite, McAfee VirusScan, and McAfee Personal Firewall, with WiFI's security solutions provides enhanced protection from malicious code and other Internet threats.

The McAfee brand is known worldwide for providing proactive security solutions, and McAfee plans to continue to develop solutions to protect customers of all sizes against evolving security threats and vulnerabilities, including blended attacks and malicious code of all kinds.

Trend Micro Inc.

Overview

Trend Micro was founded in 1988 and is headquartered in Tokyo, Japan. Its 25 business units, employing more than 2,900 people worldwide, can be found in 30 countries across Asia, Europe, North America, and South America. Trend Micro products are supported by service from TrendLabs, a global network of five regional antivirus research and support centers.

In June 2005, Trend Micro acquired Kelkea Inc., an authority on IP filtering and reputation services. This acquisition advances the opportunity for Trend Micro to develop network-level solutions against emerging and evolving threats and enhance its current antispam solutions.

Around the same time, Trend Micro also acquired InterMute Inc., a developer of antispyware products. InterMute's technology will further enhance Trend Micro's antispyware solutions for business customers and consumers.

Secure Content Management Products

Trend Micro offers the following SCM products:

- PC-cillin Internet Security provides comprehensive and easy-to-use protection from viruses, hackers, and other Internet-based threats. This consumer security solution helps to safeguard users' PCs from newly emerging threats such as network viruses, spam email, inappropriate Web content, and spyware programs that can compromise privacy.

- Trend Micro OfficeScan is a client/server security solution designed to protect against the daily threats of file-based and network viruses as well as secure access from intruders, spyware, and other threats. OfficeScan client editing gives administrators transparent access to every desktop and mobile client on the network for coordinated, automatic deployment of security policies and software updates. OfficeScan Server Edition incorporates ServerProtect technology for Windows-based servers

- Trend Micro Anti-Spyware offers consumer and enterprise environments the ability to accurately detect and remove evasive spyware and grayware in real time. Designed to operate alongside various antivirus and security software, these solutions can be used alone or as part of a layered defense strategy at multiple points in the network.

- ScanMail offers real-time virus detection and removal from emails and attachments before they reach the desktop. It integrates with Exchange and Domino. The optional eManager plug-in integrates seamlessly with ScanMail to safeguard intellectual property and confidential information, block inappropriate email and attachments, and protect against viruses. It also features optional antispam and advanced content filtering technology to ensure the uninterrupted flow of email traffic.

- InterScan Messaging Security Suite is an extensible, policy-based messaging security platform for the gateway that addresses mixed-threat attacks by delivering coordinated policies for antivirus, antispam, and content filtering.

- Spam Prevention Solution is a high-performance antispam application designed to protect the enterprise from spam at the gateway. It is integrated with the Trend Micro InterScan Messaging Security Suite, which provides comprehensive messaging security — antivirus, content filtering, and antispam — in one easy-to-manage platform.

- InterScan Web Security Suite delivers high-performance security for HTTP and FTP traffic at the Internet gateway. The suite integrates antivirus, antiphishing, antispyware, and optional URL filtering technology.

- ServerProtect provides comprehensive antivirus scanning for servers, detecting and removing viruses from files and compressed files in real time — before they reach the end user. Solutions are available for Microsoft Windows/Novell NetWare, Linux, Network Appliance filters, and EMC Celerra file servers.

Strategic Direction

Trend Micro provides its customers with security solutions that offer protection against unpredictable, malicious threats. Trend Micro pioneered innovative antivirus solutions at the server and gateway, and more recently turned its focus to providing solutions within the network layer. In addition to its software products, Trend Micro also continues to promote its service-based offerings through its Trend Micro Enterprise Protection Strategy. This initiative helps customers organize policy enforcement needs with products and services around the four primary phases of the virus outbreak life cycle: vulnerability prevention, outbreak prevention, virus response, and damage assessment and restoration.

The acquisition of Kelkea and its IP filtering and reputation services, advances the opportunity for Trend Micro to enhance its current antispam solutions and offer advanced protection against phishing, pharming, and those threats that can be launched via botnets.

The InterMute acquisition will further enhance Trend Micro's antispyware solutions for business customers and consumers. Trend Micro has already begun to offer InterMute's standalone antispyware products under the Trend Micro brand. Additionally, the company plans to integrate InterMute's antispyware capabilities into its enterprise, small and medium business, and consumer solutions.

Trend Micro also continues to collaborate with Cisco to deliver comprehensive network worm and virus outbreak-prevention technology and services to help protect networked businesses.

Computer Associates

Overview

Computer Associates was founded in 1976 and employs approximately 16,000 people worldwide. CA is headquartered in Islandia, New York, and has operations throughout the world.

Secure Content Management Products

CA offers the following SCM products:

- eTrust Secure Content Management is an integrated SCM solution that enables definition and deployment of a common enterprisewide security policy addressing HTTP, SMTP, and FTP security risks, including viruses, spam, hacking, and unacceptable use of the Web by employees.

- eTrust Antivirus provides a single, comprehensive virus management solution that eliminates virus infections, eases administration, and simplifies and automates the updating process. eTrust Antivirus covers all points of a corporate environment from the perimeter to the PDA.

- CA's eTrust PestPatrol Anti-Spyware solutions provide protection against spyware, adware and other nonviral threats. These solutions offer business-grade antispyware protection that detect and remove spyware in real time

Strategic Direction

CA's mission is to make IT simpler, more efficient, and more cost-effective. CA's Secure Content Management product line is focused on providing organizations with an integrated, policy-based content security solution that helps defend against business and network integrity threats, including spam, confidentiality breaches, exposure to email legal liability, viruses, mobile code threats, and other offensive material. eTrust Secure Content Manager allows users to create their own rules for defining spam and Web URL access. eTrust Secure Content Manager also offers business-driven policy engines, confidentiality filtering, central policy management for email and Web security, and automated alerts and actions.

eTrust Secure Content Manager builds on the strengths of eTrust Antivirus while taking content security to the next level and offering all-around protection for corporate networks. It addresses the continuing evolution of content security challenges that require a more extensive view and a larger set of solutions.

SurfControl

Overview

SurfControl is a leader in the Web and email filtering markets. It is a public company traded on the London and Nasdaq Europe exchanges. The company has more than 20,000 customers worldwide and employs nearly 530 people in 15 separate locations across the United States, Europe, and Asia/Pacific. SurfControl acquired SecureM Inc. and added a Linux-based email filter appliance technology to its product portfolio.

Secure Content Management Products

SurfControl Enterprise Protection Suite leverages the following core components to provide a proactive approach to unified threat management:

- SurfControl Web Filter defends against productivity, legal, network, and security threats by managing employee Web surfing activity. SurfControl Web Filter uses a combination of predefined URL lists and neural network technology for automatic categorization of new/unknown Web sites.

- SurfControl E-mail Filter protects enterprise email servers from multiple content threats such as spam, viruses, and junk emails (e.g., chain letters and jokes) E-mail Filter also manages email content flowing in and out of the company email system, such as confidential information and hostile or inappropriate content. Multiple technologies are used to create a gauntlet approach to identify such messages, including an antispam database that uses digital fingerprint technology, dictionaries, advanced lexical analysis, and neural networks.

- SurfControl Instant Message Filter preserves productivity and bandwidth by blocking and managing employee access to unauthorized instant message and P2P networks.

- SurfControl Enterprise Threat Shield protects networks from spyware, adware, keyloggers, instant messaging, P2P, games, and any other potentially malicious applications.

Strategic Direction

SurfControl focuses on helping companies "stop unwanted content" in the workplace by continuing to expand its product offering for filtering to address new content risk areas as they emerge. The current product set in the SurfControl total filtering solution — Web, email (including antispam and antivirus), and IM — offers a complete Web and messaging security solution. IDC believes that the solution set from SurfControl can play a key business role in intelligently filtering unwanted content and preventing it from entering an organization. By providing stronger controls on Web, IM, and email usage under a common user interface, these products provide a complementary enhancement to traditional IT perimeter security products. SurfControl recently entered the security appliance market with its acquisition of SecureM. By adding a Linux-based email filter appliance technology its product portfolio, SurfControl has strengthened its position in the Web and email filtering markets. SurfControl will expand internationally by adding a China-based sales and distribution operation.

In July of 2005, CEO and founder Steve Purdham was replaced by Patricia Sueltz, formerly of Salesforce.com. The company will remain focused on its core group of customers, businesses as opposed to consumers, with all-inclusive software suites, such as SurfControl Enterprise Protection Suite, that address the multiplying threats stemming from phishing, spyware, and viruses.

Websense

Overview

Websense was founded in 1994 and now has more than 24,000 customers. Headquartered in San Diego, California, with offices in China, Japan, and Australia and across Europe, Websense now employs approximately 530 people worldwide.

Secure Content Management Products

Websense Web Security Suite — Lockdown Edition is an integrated Web security solution that provides spyware protection and blocks access to malicious mobile code and other Web-based threats through the following:

- Websense Removable Media Lockdown allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations. Organizations can also block writable media, depending on their policy.

- Websense Network Lockdown delivers protection against known and unknown security threats by blocking application network access to specific ports and protocols by application category.

- Websense Application Lockdown provides control over desktop environments by allowing only approved applications to run on corporate PCs and servers, thereby preventing potentially malicious applications from launching. It also detects and analyzes endpoint desktop security threats and application activity.

- Websense Express Lockdown allows system administrators to prevent the execution of new applications, thereby blocking attacks such as keyloggers, Trojan horses, worms, and other malicious code threats. Unlike Application Lockdown, Express Lockdown does not require a machine inventory.

- Websense Web-based Threat Mitigation provides protection from Web-based threats, including keyloggers, spyware, Trojan horses, botnets, scripts, and ActiveX controls, via a database of malicious Web-based applications.

- Websense Enterprise manages employee Web use at three network control points: the gateway, network, and desktop. Websense Enterprise enables management across Web pages, network protocols, and desktop applications to effectively combat growing security, legal, and productivity threats that infiltrate company networks, such as P2P file sharing, IM, hacking tools, and spyware.

EXHIBIT 24

PART 2

☑ Client Policy Manager (CPM) is an innovative endpoint security solution that delivers "zero day" threat protection from unknown security threats, including today's sophisticated malware. CPM policies also stop the execution of unauthorized applications such as spyware, P2P file sharing, and hacking tools while enabling flexible policy management of applications such as IM or remote control tools that only select users are allowed to launch. CPM also allows organizations to lock down removable media such as flash drives, CD/DVD burners, floppy drives, and external hard drives to avoid use on client workstations. Utilizing a unique application database with more than 50 categories, CPM enforces flexible-use policies for corporate desktops, mobile laptops, and servers.

☑ Bandwidth Optimizer improves overall network performance by reducing the use of non-work-related, high-bandwidth media based on real-time network conditions.

☑ IM Attachment Manager is an add-on module that enables IT managers to control the sending and receiving of files via IM clients. This module controls the security and legal risks posed by the unmanaged use of IM attachments, and it helps optimize IT resource allocation and employee productivity.

Strategic Direction

Websense was a leader in Web filtering revenue for 2004. Websense provides a layered solution to help organizations address Web security concerns by blocking access to spyware Web sites and spyware back-channel communication at the gateway and by preventing spyware applications from launching at the desktop. Websense secures organizations from emerging Internet threats by providing a Web security component that complements traditional security solutions.

Websense Web Security Suite provides an integrated Web security solution that offers spyware protection and blocks malicious mobile code and other Web-based threats as well as spyware and keylogging transmissions back to their host sites. It also protects employees from phishing and controls the sending and receiving of IM clients. The Websense Web Security Suite provides real-time Internet security updates for protection from new security threats and includes reporting and analysis tools that provide organizations with information on user access to fraudulent sites or vulnerability to malicious code.

Websense recently announced the general availability of Websense Enterprise CPM, a desktop security solution that fills critical endpoint gaps in today's multilayered enterprise defense systems. Complementing traditional firewall and antivirus tools, CPM closes the window of exposure to unknown security threats that often bring down networks before a virus signature or vulnerability patch is deployed.

Sophos

Overview

Sophos is a security specialist, developing software against viruses, spyware, spam, and policy abuse. The company protects businesses and organizations against viruses and spam. Founded in 1985, Sophos is privately owned, with headquarters in the United Kingdom and approximately 1,000 employees worldwide. It also has subsidiaries throughout the world — in the United States and Australia and throughout Europe, Japan, and Singapore.

Secure Content Management Products

Sophos offers the following SCM products:

☒ Sophos Anti-Virus software offers multiple-platform support for the enterprise, small businesses, and academic institutions. It protects laptops, desktops, and servers by detecting, reporting, and disinfecting viruses. Scheduled and on-demand scanning is provided by Sophos' proprietary virus detection engine.

☒ Sophos PureMessage is a comprehensive, secure mail filtering solution for email servers, protecting them against viruses, spam, and other email-borne security threats. It combines antivirus and antispam technologies with flexible policy management.

☒ Sophos MailMonitor protects corporate networks at the email gateway, reducing the significant threat of email-borne viruses. All traffic passing through gateways and email servers is checked, and any potential carriers are blocked and quarantined. Sophos' threat-reduction technology can address future threats by blocking all attachments with executable code.

☒ Sophos ZombieAlert is a subscription support service that identifies and alerts organizations to zombie computers on the network. Zombie computers are infected machines that give control to unauthorized and remote users, allowing them to send spam from the computer or to launch email-based denial-of-service attacks against Web sites. Sophos ZombieAlert offers a global network of threat analysis centers, providing around-the-clock visibility into new and emerging threats, including compromised computers. This alert service gives organizations the opportunity to remedy the situation and clean their systems.

Strategic Direction

Sophos provides virus and spam solutions for organizations of any size, from large enterprises to small businesses. Sophos' strategic direction focuses on long-term cost-of-ownership reduction. Sophos is the only secure content management solutions provider covered in this study that is focused solely on the enterprise market. The company's products are sold and supported through a global network of subsidiaries and partners in more than 150 countries. In addition, virus and spam experts based at Sophos' high-security research laboratories in the United Kingdom, the United States, Canada, and Australia carry out 24-hour analysis to ensure rapid response to any new threat anywhere in the world, irrespective of time zone.

In January of 2005, Sophos joined the Network Appliance partner program as an Advantage Partner. Sophos Anti-Virus for NetApp storage systems scans regularly for viruses and other malicious software in order to protect critical business information. Sophos' solution scans at the storage level rather than the user level to improve file access speed. Sophos Anti-Virus is optimized for all NetApp storage systems running the Data ONTAP operating system and can administer remote scans through any Windows NT/XP/2000/2003 computer. Sophos for NetApp storage systems can also be configured to update automatically to reduce the load on IT administrators while ensuring the most up-to-date network security.

Driven by mounting pressures to ensure a secure and low-cost infrastructure, Sophos will continue to focus on providing consolidated protection against security threats such as viruses, spam, and policy breaches.

Clearswift

Overview

Clearswift, the MIMEsweeper company, is present in 15 countries worldwide with headquarters both in the United Kingdom and the United States and sales offices in Germany, Japan, and Australia. Clearswift has 15,000 customers and is a leading supplier of content security software for email and the Web.

Secure Content Management Products

Clearswift offers the following SCM products:

☒ MIMEsweeper SMTP Appliance is a preloaded appliance offering antivirus, antispam, antispyware, antiphishing, "plug and play" deployment, automated updates, and easy management of both inbound and outbound filtering and content compliance. It performs policy-driven email content security to help protect against loss of intellectual property and safeguard the privacy of organizations and individuals as electronic content is transferred in, out, and around organizations.

☒ MIMEsweeper for SMTP is an external email solution that protects organizations against inbound and outbound email threats, from spam and viruses to employee time wasting, circulation of pornography, breaches in confidentiality, legal liability, and IT resource misuse.

☒ MIMEsweeper for Web brings policy-based content security to the HTTP gateway. MIMEsweeper for Web analyzes Web content and blocks pages or files that are prohibited by an organization's security policy. It also provides policy-based content security for organizations that allow access to Web-based email.

☒ MIMEsweeper for Exchange and MIMEsweeper for Domino provide internal email security for organizations protecting against harassment and the advertant and inadvertent distribution of confidential information.

Strategic Direction

Clearswift secures content and protects against digital attacks by enforcing security policies that increase productivity, reduce IT costs, and create a safer business environment. Its goal is to provide total content security for email and Web. Clearswift's core expertise lies in the content analysis and policy enforcement of email and Web content traveling into, across, and out of organizations. Clearswift enables organizations to protect themselves against digital attacks, meet legal and regulatory requirements, implement productivity-saving policies, and manage intellectual property passing through their networks. MIMEsweeper for SMTP 5.1 provides a content analysis engine that allows organizations to filter inbound and outbound traffic according to a variety of attributes. Each email and attachment that comes into or leaves a company's internal network is scanned and compared against the personalized policy to ensure that information is appropriate. It is now available in a preloaded appliance offering "plug and play" deployment, automated updates, and easy, intuitive management.

Clearswift meets the overwhelming demands of the market to address regulatory and legal issues brought on by regulatory statutes and compliance laws worldwide. Underpinning the strategic road map, Clearswift will provide content security solutions to the market on a range of platforms — software, managed services, and appliances. Clearswift's road map is focused on helping organizations address the future of the rapidly changing Internet and email content security market.

MessageLabs

Overview

MessageLabs is a privately held company that provides managed email security services to businesses. The company has more than 12,000 clients worldwide, including the British government, The Bank of New York, EMI Music, HealthPartners, StorageTek, Air Products and Chemicals, SC Johnson, Conde Nast Publications, Fujitsu, and Diageo. MessageLabs is headquartered in Gloucester, the United Kingdom, and has offices throughout the United Kingdom, the United States, Hong Kong, Singapore, Australia, Belgium, and the Netherlands. MessageLabs recently partnered with ScanSafe to offer new Web filtering services.

Secure Content Management Products

MessageLabs offers the following SCM products:

- Skeptic is the heart of MessageLabs' email security solution. Skeptic uses patented artificial intelligence and learning from an ever-expanding knowledge base of email security threats to identify viruses, spam, and pornography without the need for time-delayed updates like with traditional software.

- MessageLabs' Anti-Virus Service combats known and unknown viruses, trojans, and other forms of malware before they reach an organization's network. The service uses multiple scanners and predictive technology, includes a 100% service-level agreement, and has protected thousands of organizations from major outbreaks during the critical period before signatures are available.

☒ MessageLabs' Anti-Spam Service is a comprehensive solution for combating unsolicited bulk email and stopping it from reaching an organization's network while ensuring legitimate messages are delivered accurately, using a combination of predictive technology, third-party software, signature management, and client-configurable approved and blocked sender lists.

☒ The MessageLabs Image Control Service scans and detects inappropriate content in inbound and outbound email using Image Composition Analysis to detect pornographic and other unwanted images for enforcement of email acceptable usage policies.

☒ The MessageLabs Content Control Service enables organizations to identify and control confidential, malicious, or inappropriate content sent or received by their organization using textual scanning, lexical analysis, and attachment controls.

☒ MessageLabs Boundary Encryption offers organizations the ability to set up a secure private email network between themselves and their partners to ensure the end-to-end delivery of encrypted communications without the need for complicated hardware or software to set up, configure, or maintain.

Strategic Direction

The MessageLabs vision is purely and simply to be the premier provider worldwide of business email security and management services. MessageLabs believes the most effective solution is one that sits outside the corporate network and can eliminate email threats, both inbound and outbound, outside the boundaries of the corporate network and before they reach critical corporate systems. The company's centralized managed service model draws on significant economies of scale to give organizations a high-quality service with complete interoperability with existing systems, 24 x 7 service and support, email attack, and denial-of-service protection while requiring no additional investments in hardware or software. The MessageLabs services are powered by a global network of 13 datacenters built on a secure, scalable architecture, capable of handling millions of emails every day.

MessageLabs and IBM Global Services recently announced a partnership to help companies fight the growing financial, legal, and technical damages posed by spam, unwanted images, and viruses in email that cost businesses billions of dollars a year. The companies offer antispam, antivirus, and image control services to businesses worldwide as part of IBM's Managed Security Services, Email Security solutions. IBM offers MessageLabs' services as part of the company's broader security portfolio, which includes intrusion detection, firewall management, antivirus management, vulnerability scanning, and incident management services.

A recent partnership with ScanSafe has facilitated the upcoming introduction of a new MessageLabs Web filtering service in October 2005. MessageLabs holds a minority interest in the London-based company, which also sells the Web filtering services on its own. The Web filtering service will allow the scanning of Web traffic for viruses, spyware, and adware. It will also allow filtering and Web site blocking by routing Web traffic through a MessageLabs datacenter. MessageLabs also has partnerships with

MCI, Unisys, CSC, Cable & Wireless, BT, Paetec, IntelliSpace, Eureka Networks, and hundreds of other companies, which are helping MessageLabs expand its global reach and market share.

Tumbleweed Communications

Overview

Tumbleweed Communications Corp. was founded in 1993 and held its initial public offering in 1999. The company has over 300 employees around the world and is headquartered in Redwood City, California, with offices in Hong Kong, Singapore, New Zealand, and across Europe. The company is trusted by over 1,200 enterprise customers around the world who use Tumbleweed products to connect with over ten thousand corporations and millions of end users.

Secure Content Management Products

Tumbleweed Communications offers the following SCM products:

- Tumbleweed MailGate Appliance is a comprehensive email security product offering antispam, antiphishing, antivirus, antispyware, network edge defense, custom policy management, content filtering, and encryption in an easy-to-install and manage appliance. With flexible deployment options including a modular design and centralized management and reporting, the MailGate Appliance fits into any IT infrastructure and can scale to any size environment.

- Tumbleweed MailGate Email Firewall is a comprehensive email security product offering antispam, antiphishing, antivirus, custom policy management, content filtering, and encryption in a flexible, configurable software form factor. In addition to protecting companies against a wide range of incoming email threats, MailGate Email Firewall lets organizations enforce corporate policies to encrypt or block outgoing email to safeguard proprietary information, and comply with industry and government regulations.

- Tumbleweed MailGate Secure Messenger is an email encryption server. Currently deployed at some of the most demanding enterprises in the Global 2000, MailGate Secure Messenger enables organizations to meet their own unique security needs — from compliance with government privacy regulations in healthcare (HIPAA) and financial services (GLBA) to enforcement of corporate policies (SOX) and protection of intellectual property.

- Tumbleweed SecureTransport is an enterpriseclass managed file transfer solution for moving financial transactions, critical business files, large documents, XML, and EDI transactions over the Internet and private IP networks. Deployed at over 20,000 sites around the world, SecureTransport is used to move billions of dollars in financial transactions daily. Nine of the top 10 U.S. banks use it to serve tens of thousands of corporate customers; healthcare networks use it to provide a single, integrated file transfer infrastructure for securely exchanging private health information (PHI); and government agencies use it to share sensitive documents with other agencies.

Strategic Direction

Tumbleweed provides secure Internet communications solutions for enterprises and government customers of all sizes, allowing them to safely and efficiently leverage these communication channels to optimize and grow their businesses. Tumbleweed offers these security solutions in three comprehensive product suites: MailGate, SecureTransport, and Validation Authority. MailGate provides protection against spam, viruses, and attacks and enables policy-based message filtering, encryption, and routing. SecureTransport enables organizations to securely and reliably exchange data and files with their customers and partners over the Internet. Validation Authority is the world-leading solution for determining the validity of digital certificates.

In July of 2005, Tumbleweed named Craig Brennan chairman and CEO. Brennan takes over from founder and former chairman Jeff Smith, who remains on Tumbleweed's board. In 2Q05, Tumbleweed announced record revenues. The company's investments to strengthen product offerings and initiatives to expand distribution channels paid off with a 40% increase in new orders year over year, more than 100 new customers, and a doubling of the revenues received from channel partners quarter over quarter.

F-Secure

Overview

Founded in 1988, F-Secure Corp. has been listed on the Helsinki Stock Exchange since November 1999. The company is headquartered in Helsinki, Finland, with country offices in the United States, France, Germany, Italy, Norway, Poland, Singapore, Sweden, the United Kingdom, and Japan.

Secure Content Management Products

F-Secure offers the following SCM products:

☑ F-Secure Anti-Virus suite products include all critical components for corporate virus security for laptops, desktops, file servers, email servers, and gateways. All F-Secure products can be centrally managed with F-Secure Policy Manager.

☑ F-Secure Anti-Virus Client Security is a centrally-managed solution consisting of tightly-integrated virus protection, spyware protection, desktop firewall, and intrusion prevention and application control software for desktop and laptop computers. The solution is available for both Windows and Linux operating systems.

☑ F-Secure Anti-Virus for Workstations and File Servers protects laptops, desktops, and file servers against viruses and malicious code in real time. It protects both site-based and mobile workers ensuring maximum system availability and data integrity. The solution is available for both Windows and Linux operating systems. F-Secure Anti-Virus Mail Server and Gateway products provide powerful and easy-to-deploy virus protection solutions for industry standard firewalls, groupware, and email environments.

- F-Secure Messaging Security Gateway delivers comprehensive and effective security for email It combines a robust, enterpriseclass messaging platform with perimeter security, antispam, antivirus, secure messaging, and outbound content security capabilities in an easy-to-deploy, hardened appliance.

- F-Secure Mobile Anti-Virus is a comprehensive solution for protecting mobile devices against viruses and other harmful content. It provides real-time on-device protection with automatic over-the-air antivirus updates through a patented SMS update mechanism or HTTPS connections and centralized subscription management for corporations. F-Secure also offers security solutions to mobile operators to ensure security in their network and subscribers' terminals

- F-Secure consumer products include F-Secure Anti-Spyware, F-Secure Anti-Virus 2006, and F-Secure Internet Security 2006. F-Secure Internet Security is an all-in-one security suite that offers complete protection against Internet threats. It contains a real-time antivirus and antispyware coupled with a firewall, antispam and parental control

Strategic Direction

F-Secure protects individuals and businesses against computer viruses and other threats spreading through the Internet and mobile networks. F-Secure is a pioneer in creating security applications that are optimized for wireless devices and offer reliable and automatic on-device protection. F-Secure Anti-Virus ensures complete protection for handheld devices. The company also offers security solutions for mobile operators and service providers. F-Secure is supported by a global ecosystem of VARs and distributors in more than 50 countries. F-Secure protection is also available through major ISPs such as Deutsche Telekom and leading mobile equipment manufacturers such as Nokia.

F-Secure's key strength is its proven speed of response to new threats. F-Secure recently announced the launch of the industry's first Mobile Anti-Virus product in a box for the retail market. The retail box product is targeted principally for consumers as well as for small and medium-sized businesses. F-Secure anticipates increasing threats from mobile malware and wants to position its products before these threats reach the levels witnessed in the PC world.

F-Secure believes that its new mobile and wireless products and services, combined with a solid history in the antivirus market, will put the company in a strong position to lead the mobile operator business, especially in Europe, in 2005.

Secure Computing

Overview

Secure Computing Corp. was founded in 1984 as a division of Honeywell and had its initial public offering in 1995. The company is headquartered in San Jose, California, and has sales offices throughout the United States and in the United Kingdom, France, Germany, Singapore, Hong Kong, Japan, and Australia. In August of 2005, Secure Computing announced its plans to acquire CyberGuard, a global provider of security solutions that protect the business-critical information assets of Global 2000 enterprises and government organizations. The acquisition of CyberGuard will allow Secure Computing to solidify its presence in the secure content management market with the adaptation of CyberGuard's Webwasher products.

Secure Content Management Products

Secure Computing offers the following SCM products:

☒ SmartFilter is a Web filtering solution that is used by companies to safeguard work environments from offensive content, limit legal liability, and protect against malicious code that can enter networks when employees use the Internet.

☒ SmartFilter, Bess edition is used by K–12 schools to cost-effectively protect students from inappropriate or illegal Internet content. CIPA-compliant and easy to use, Bess delivers the only true education-centric filtering solution in the business.

Strategic Direction

Secure Computing sells specific solutions to address the varying needs of organizations of all sizes and educational institutions. Secure sells on a global basis primarily via distributors, VARs, and resellers to enterprise, government, and education customers and as well through a network of brand name OEMs.

The Secure Computing business model of delivering its SmartFilter on-box Web filtering solution to the marketplace is unique in its heavy emphasis on an OEM model. Market-leading OEM partners such as Cisco, Blue Coat, Network Appliance, McAfee, and CA represent the primary mechanism for delivering the SmartFilter software and control list to the marketplace.

The acquisition of CyberGuard and its Webwasher products allows Secure Computing to leverage and extend its market coverage. The products offered in the Webwasher CSM Suite provide a filtering solution implemented at the corporate gateway, integrating and enhancing existing IT infrastructure to optimize Internet usage and protecting against threats arising from the Internet. Webwasher brings another means of selling Web filtering to Secure Computing, which has an absence in the area of standalone appliance-based nondependency solutions for Web filtering.

The CyberGuard acquisition is expected to be final by November 2005. Secure Computing expects there will be no rapid changes in its offerings and plans to maintain support for all CyberGuard products currently on the market.

Secure Computing will have a wider and denser sales coverage with the CyberGuard acquisition because the majority of Secure Computing revenue is from within the United States, while CyberGuard's revenue is primarily from outside of the United States. By combining the strengths and complementary aspects of Secure Computing and CyberGuard, the company is consolidating its presence in the secure content management and Web filtering market.

Webwasher

Overview

Webwasher AG was founded in 1999 as a Siemens spin-off and is headquartered in Paderborn, Germany. On April 26, 2004, CyberGuard announced that it had acquired Webwasher. Most recently, CyberGuard was acquired by Secure Computing to unify its presence in the threat management market. IDC believes Webwasher will remain a separate business unit inside Secure Computing.

Secure Content Management Products

Webwasher offers the following SCM products:

- Webwasher URL Filter wards off security, productivity, and legal threats arising from the Web at the corporate gateway in a comprehensive and highly efficient manner, also giving protection against spyware and phishing attacks. In a dual approach, it uses both a static scanning method relying on a large-scale URL database and real-time scanning of uncategorized URLs. Content filtering and blocking are enhanced by a proficient media type filter, limiting, for example, the downloading of voluminous audio and video files.

- Webwasher Antivirus is a filtering solution combining proactive and pattern-based methods to monitor Web and email communication and deliver the security necessary to ensure unimpeded performance of business-critical processes. The solution implements the unique Webwasher Antivirus PreScan technology to accelerate scanning, providing risk-free Web usage with a very low latency time.

- Webwasher Anti Spam offers accurate spam detection and prevention for Web and email communication. To improve the quality of the spam classification process, Webwasher's MethodMix filtering technology is applied, where several complementary methods operate and achieve their results simultaneously or in any desired combination. Queue management permits the professional handling of blocked items, as is especially required in larger organizations.

- Webwasher Content Protection offers protection against threats emanating from sources such as scripts, embedded objects, ActiveX, document macros, and Java applets and prevents leakage of confidential content in outgoing traffic. The filters included are based on a series of customizable response actions and settings, allowing for the creation of a companywide content security policy.

- Webwasher SSL Scanner extends existing Web-based content security measures to the HTTPS, allowing normal content and security filters to be applied to originally encrypted content. Decryption is possible at the gateway as a result of certificate-based coordination between the employee's browser and the corporate Web gateway/proxy.

- Webwasher Instant Message Filter detects, reports, and selectively blocks the unauthorized use of high-risk and evasive P2P file sharing and instant messaging from enterprise networks.

☒ Webwasher Content Reporter is Webwasher's premium reporting tool for Internet policy compliance, cache performance, and streaming media statistics as well as Web and email activity.

Strategic Direction

Webwasher is a leading provider of Internet security solutions for companies and public institutions. On the basis of its own technology developments as well as by cooperating with leading technology partners, the company develops and markets innovative products for the growing content security management market.

The products, offered in the Webwasher CSM Suite, provide a comprehensive filtering solution implemented at the corporate gateway, integrating and enhancing existing IT infrastructure to optimize Internet usage and give protection against threats and annoyances arising from the Internet. The products feature Web, email, instant messaging, and spam filtering, as well as virus protection, centralized policy and reporting management, and single-installation deployment.

The acquisition of CyberGuard and its Webwasher products allows Secure Computing to leverage and extend its market coverage. The products offered in the Webwasher CSM Suite provide a filtering solution implemented at the corporate gateway, integrating and enhancing existing IT infrastructure to optimize Internet usage and protecting against threats arising from the Internet. Webwasher brings another means of selling Web filtering to Secure Computing, which has an absence in the area of standalone appliance-based nondependency solutions for Web filtering.

CipherTrust Inc.

Overview

Headquartered in Atlanta, CipherTrust Inc. is a global messaging security company dedicated to developing comprehensive layered security solutions for corporate messaging systems to stop inbound email threats such as spam, viruses, intrusions, spyware, zombies, and phishing and protect against outbound policy and compliance violations. CipherTrust protects the messaging systems of 1,800 organizations in 40 countries worldwide, including more than a third of the Fortune 500.

Secure Content Management Products

CipherTrust offers the following SCM products:

☒ CipherTrust provides a comprehensive, layered approach to protecting corporate messaging systems. At the core of this protection is CipherTrust's TrustedSource global threat correlation engine, which provides reputation scores for email senders based on various behavior techniques. TrustedSource analyzes more than 10 billion messages per month from CipherTrust's global network of enterprise customers.

☒ Powered by CipherTrust's TrustedSource global threat correlation engine, the Company's flagship offering, IronMail Gateway, provides comprehensive inbound threat protection and protects against outbound policy and compliance violations. The IronMail Gateway is available in the S-Class version for small and medium-sized organizations, the E-Class version for large enterprises, and the C-Class version for carriers, ISPs, and multinational corporations with several geographically dispersed gateways.

- Powered by CipherTrust's global threat correlation engine, the IronMail Edge appliance provides an outer layer of security at the network perimeter to protect against malicious email threats before they hit any part of an enterprise network. IronMail Edge can handle three million messages per hour and effectively reject more than 50% of email connections by identifying them as being from a malicious source.

- CipherTrust's IronMail Encryption provides policy-based, flexible protection against outbound policy and compliance violations. Its policy-driven approach allows enterprises to define their own policies and automatically enforce these policies across the organization, including enabling messages to automatically block, encrypt, carbon copy, route, and so forth. The offering also includes its Secure Web Delivery staging server capability

- CipherTrust's IronMail Compliance Control allows organizations to set policies that easily and automatically manage noncompliant messages as soon as they are detected. Because it is policy driven, most functions are automated. The exceptions are handled directly by the decision maker (compliance officer), rather than relying on an intermediary (administrator) to interpret rules made by another party.

- CipherTrust's Hosted IronMail is designed for those organizations without the resources or expertise to manage the complexities of email security. Hosted IronMail provides all the benefits of IronMail Gateway for those organizations that prefer to outsource the management of their email security.

- CipherTrust's TrustedSource Portal is a free online resource that provides precise information about email sender reputation by domain and IP address. Located at **www.trustedsource.org**, the TrustedSource Portal is the only Web site in the world that provides a single view of senders using one or more of the four primary email authentication standards designed to minimize phishing, fraud, and spam: DomainKeys and DomainKeys Identified Mail (DKIM) advocated by Cisco and Yahoo and SenderID and Sender Policy Framework (SPF) advocated by Microsoft.

Strategic Direction

CipherTrust pioneered the messaging security industry in 2000, when an email expert and leading security specialist detected the market opportunity for an email security appliance. The company developed IronMail to help customers predict, identify, and solve critical email security issues with industry-leading knowledge and state-of-the-art technology. Over the years, CipherTrust has evolved its comprehensive layered approach to protecting the messaging systems of today's enterprises.

The company's flagship IronMail Gateway provides multiple integrated solutions on a single appliance, complete with the added benefit of common policy. CipherTrust is well positioned to develop and implement comprehensive policy-based protection for all messaging protocols (including email, instant messaging, and wireless) and against evolving threats (including spam, virus, phishing, spyware, and zombies). CipherTrust offers a comprehensive layered security approach at the edge, gateway, and at the desktop. Today, CipherTrust offers end-user quarantines and will extend more functionality to the end user to be able to report spam and check reputation using its TrustedSource global threat correlation engine, the most advanced, precise sender reputation system in the world

CipherTrust also provides comprehensive, flexible outbound compliance and encryption capabilities via proprietary technology as well as integrated, best-of-breed technology partnerships. Overall, the company continues to increase effectiveness while reducing the total administration time companies spend on managing and securing their inbound and outbound messaging infrastructures.

Aladdin Knowledge Systems

Overview

Aladdin Knowledge Systems (Nasdaq: ALDN) has been providing strong network and software commerce security solutions since 1985. Employing more than 350 people worldwide, Aladdin is headquartered in Arlington Heights, Illinois, with locations in Israel, the United Kingdom, Japan, and Europe. It services more than 30,000 customers.

Secure Content Management Products

Aladdin Knowledge Systems offers the following SCM products:

- eSafe Gateway is a comprehensive solution providing a high-capacity, proactive, real-time, and multitier content security and antispam solution for the Internet gateway.

- The eSafe Mail solution provides email content and attachment security, with proactive antivirus and antispam capabilities optimized for enterprise network email servers.

- The eSafe Appliance is the platform-independent version of eSafe Gateway delivered as a preconfigured plug-and-play CD ready with hardened Linux OS and available installed on Aladdin hardware.

Strategic Direction

Aladdin is focused on providing integrated proactive content security solutions to combat the ever-growing number of blended threats. eSafe's new application filtering technology, called AppliFilter, effectively blocks P2P, IM, spyware, adware, tunneling, and other unauthorized application traffic. eSafe's AppliFilter stops these applications from circumventing firewall systems and infiltrating an organization. Aladdin's HASP products offer software and intellectual property protection. This pioneering approach of integrating the application filtering technology in a gateway-based content security solution is positioned to change the way organizations view perimeter security.

eSafe's AppliFilter technology is based on a sophisticated auto-updating engine that monitors all opened connections, looking for unauthorized applications and protocols patterns within the request and response TCP/IP traffic. AppliFilter is designed to enhance traditional network-level firewalls and provide application-layer protection against immediate threats.

NetIQ

Overview

NetIQ is headquartered in San Jose, California; has operations across the United States; and sells its products to more than 60,000 customers worldwide. NetIQ is a provider of systems management, security management, Windows administration, and Web analytics solutions.

Secure Content Management Products

NetIQ offers the following SCM products:

☒ NetIQ MailMarshal is an external email security solution that scans the content of all mail messages for virus and spam characteristics. It blocks spam and cleans viruses from messages.

☒ NetIQ WebMarshal is a Web filtering solution designed to ensure protection and productivity when it comes to corporate Web use. It blocks users from within a corporate intranet from accessing a predefined list of banned sites and scans file downloads for viruses.

Strategic Direction

NetIQ MailMarshal offers comprehensive security solutions designed to secure and manage email and Web activity. NetIQ's Content Security products filter out common email security threats such as spam, viruses, and malicious code. NetIQ addresses a leading problem faced by email administrators today — the controlling of spam and the monitoring of electronic data entering and leaving the organization — and adds content security to NetIQ's comprehensive range of migration, security administration, and performance management solutions for messaging environments. Marshal Content Security Solutions from NetIQ help protect against threats to network and information security, workplace liability issues, unnecessary bandwidth consumption, and worker unproductivity associated with uncontrolled use of the Internet.

Finjan Software

Overview

Finjan was founded in 1996 and is headquartered in San Jose, California, with additional offices in the United States, Europe, Asia Pacific, and the Middle East. It offers security solutions to companies of all sizes (from SMB to large enterprises). It services, among others, the finance, banking, insurance, healthcare, airlines, and high-technology sectors and large government agencies.

Secure Content Management Products

Finjan offers the following SCM products:

- The Vital Security Appliance Series NG-5000 and Series NG-8000 are Finjan's next generation content security platforms, comprising an advanced set of robust, hardware-based security solutions for enterprises. Integrating Finjan's patented Next Generation Application-Level Behavior Blocking, Vulnerability Anti.dote and Anti-Spyware with best-of-breed antivirus, antispam, and URL filtering engines, Finjan's enterprise solutions provide day-zero protection against both known and unknown attacks from Web and email traffic. Finjan offers these solutions in a series of cost-effective, ready-to-use, high performance appliances. In addition, Finjan offers a dedicated Anti-Spyware Gateway Appliance for enterprises that require a standalone antispyware solution with minimal management overhead.

- Vital Security Appliance NG-1100 is Finjan's next generation offering for Web security, comprising Next Generation Application-Level Behavior Blocking, Vulnerability Anti.dote, Anti-Spyware, and best-of-breed third party antivirus and URL filtering engines. Using combinations of these modules, small and medium-sized businesses can build an integrated solution based on their specific needs.

- Vital Security Appliance NG-1400 enables threat analysis of encrypted SSL/HTTPS traffic and enforces SSL certification. NG-1400 decrypts SSL/HTTPS traffic and reveals the original data, allowing NG-1100 or another Web security proxy to perform security analysis and defend against hidden attacks.

- Vital Security Appliance NG-1700 is a dedicated antispyware gateway appliance for SMBs, based on a single security policy optimized to block known and unknown spyware, which enables quick "plug and play" installation and minimal maintenance.

- The 1Box Series of appliances are specially designed for small and medium-sized businesses. Internet 1Box is a comprehensive content security solution for Web and email at the gateway and desktop, protecting against known and unknown threats. Documents 1Box is a secured document sharing and publishing solution in the SMB space.

Strategic Direction

Finjan Software, the inventor of proactive content behavior inspection, protects organizations using its Next Generation of Vital Security Appliance Series of products that provide day-zero defense against new, previously unknown attacks by leveraging its proprietary application-level behavior blocking technology.

Finjan recently unveiled its dedicated Anti-Spyware Gateway Appliance, which detects unknown and targeted spyware attacks and blocks them before they infiltrate company networks. The plug-and-play appliances are offered for small to medium-sized businesses and midrange enterprises.

Believing that security is best achieved through multiple layers of protection, Finjan's Vital Security Appliance Series NG platform offers an integrated best-in-breed solution suite of proactive, behavior-based, and traditional security technologies, including proactive malicious mobile code and active content defense, traditional antivirus protection, antispam defense, URL filtering, HTTPS/SSL traffic scanning, digital watermarking, and DRM.

As a leading innovator in the proactive content security space, Finjan is committed to providing its customers with the most advanced technology solutions to ensure day-zero security. Currently, Finjan has eight technology patents with various others pending. Finjan's Malicious Code Research Center (MCRC) specializes in the discovery and analysis of new vulnerabilities that could be exploited for Internet and email attacks Using this expertise, MCRC researchers contribute to the development of Finjan's next-generation products to keep Finjan customers protected from the next, yet-to-be-discovered attacks, as well as work with the world's leading software vendors to patch their security holes.

Blue Coat Systems

Overview

Blue Coat was founded in 1996 as CacheFlow Inc. and is headquartered in Sunnyvale, California. The company makes wire-speed proxy appliances that provide visibility and control of Web communications and has more than 3,500 customers worldwide. In November 2004, Blue Coat acquired Cerberian, a provider of URL filtering software.

Secure Content Management Products

Blue Coat offers the following SCM products:

☒ The ProxySG 800 and the ProxySG 8000 were designed to meet enterprise requirements for capacity, performance, availability, and centralized management. Although all three provide the same broad application support and features, the 8000 Series provides an expandable, modular platform for customizing disk size, RAM, and network interface cards.

☒ The ProxySG 400 enables corporations to extend Web traffic protection and control to the network edge while significantly reducing the administration and management costs for securing a distributed enterprise.

☒ The ProxyAV 400 and 2000 Series appliances enable organizations to deploy Web antivirus with scalable, high-performance options that meet the real-time requirements of Web traffic. The ProxyAV works with Blue Coat's ProxySG platform to quickly and intelligently process Web objects for Web virus scanning performance.

- ☒ Blue Coat Spyware Interceptor is an antispyware appliance for networks of up to 1,000 users. Interceptor's SCOPE antispyware engine employs 10 methods of protection daily to prevent known and unknown spyware while enabling legitimate applications.

- ☒ Blue Coat WebFilter is an on-proxy URL filter that protects Internet threat and abuses from spyware, adware, shareware, malware, P2P, IM, and pornography.

Strategic Direction

The Blue Coat ProxySG family of proxy appliances provides visibility and control of Web communications with wire-speed performance. Based on Blue Coat SGOS, a custom, object-based operating system with integrated caching, these proxy appliances leverage existing authentication systems to enable flexible policy enforcement down to the individual user. Blue Coat also makes the ProxyAV appliance for scalable, high-performance Web antivirus. The ProxyAV works with the Blue Coat ProxySG to quickly and intelligently process Web objects and determine which objects should be scanned for viruses. The product also leverages caching and heuristic fingerprinting as an additional performance benefit to deliver real-time Web traffic virus scanning.

The acquisition of Cerberian enables Blue Coat to integrate Cerberian's URL filtering and categorization technology into the Blue Coat ProxySG appliances. Blue Coat continues to support on-proxy URL filtering with databases from Secure Computing, SurfControl, Websense, and ISS, providing customers with continued flexibility to choose among each of the databases.

Under the terms of the deal, Blue Coat will continue to support Cerberian's original equipment manufacturer relationships and has assumed all customer support obligations to provide a smooth transition for all users.

Blue Coat partners with a range of leading technology companies and systems integrators to provide complete solutions for its customers. Current technology partners include Secure Computing, SurfControl, and Websense for URL filtering and Finjan, McAfee, Panda, Sophos, Symantec, and Trend Micro for Web virus scanning. Additionally, Blue Coat has a global network of distribution and channel sales partners.

Sendmail

Overview

Sendmail Inc. was founded in 1988 with the mission of providing trusted email communications. It serves more than 4,500 customers worldwide, including more than 1,000 professional services implementations for large, distributed enterprises with highly complex messaging networks. Sendmail has corporate headquarters in Emeryville, California, and offices in North America, Europe, and Asia.

Secure Content Management Products

Sendmail offers the following SCM products:

- Mailstream Manager offers antispam, antivirus, and mail policy enforcement in one centrally managed solution to protect an organization's network from security threats.

- Workforce Mail is based on the Mailstream Manager platform, but offers email scanning and defense to the deskless worker.

- The Sendmail Sentrion email gateway security appliance delivers the latest in spam and virus protection, defends against denial-of service attacks, and easily enforces the most complex business rules.

Strategic Direction

Sendmail provides comprehensive control of the mail stream and of the messaging system, protecting against spam, viruses, and intrusion while giving legitimate users secure message access. Sendmail's Content Management Filters, leveraging the unique API built into the Sendmail MTA, allow comprehensive policy-based control of data passing through the system to limit liability, scan for viruses, protect sensitive data, and enable regulatory compliance and policy enforcement. Powerful, intuitive interfaces and tools make installation, configuration, and account and data management easy and secure, lowering administrative costs and speeding deployment.

Sendmail serves more than 4,500 customers worldwide, including more than 1,000 professional services implementations for large, distributed enterprises with highly complex messaging networks. Sendmail customers represent the leaders in financial services, healthcare, communications, government, technology, and other global-scale markets

Sendmail recently announced availability of its latest advance in email security, Sendmail Sentrion. Sentrion addresses the growing demand for an email gateway security appliance that is capable of handling high message volumes, defending against emerging threats, managing strict regulatory demands, and creating policy that evolves with changing business needs — all while reducing the administration burden on IT. Sendmail gives enterprises the latest advance in email security by offering an appliance designed to work as either a standalone gateway appliance at the network perimeter, or as part of an integrated enterprise software and appliance solution that provides total protection from the enterprise gateway to the mailbox.

Sigaba

Overview

Secure Data in Motion (DBA Sigaba) is headquartered in San Mateo, California. Originally founded in 2000, Sigaba has offices in major cities across North America. Sigaba is privately held, with funding from Liberty Partners and Royal Wulff Ventures.

Secure Content Management Products

Sigaba offers the following SCM products:

- Sigaba Secure Email secures emails automatically, based on enterprisewide policies. The system enables administrators to enforce a wide variety of policies, such as encryption, virus scanning, content filtering, archiving, and quarantining. Policies are enforced at the server, gateway, and desktop.
- Sigaba Secure Instant Messaging scans and monitors IM exchange both in the corporate intranet and with external users, prevents the transmittal of viruses and spam, and enforces enterprisewide policies, including archiving, auditing, transcribing, end-to-end encryption, and digital signatures
- Sigaba Secure Statements ensures that electronic statements comply with GLS and HIPAA regulations for privacy. It provides secure delivery with distributed key technology, true authentication, fraud checks, and a robust audit trail.

Strategic Direction

Sigaba solutions enable organizations to experience the benefits of the Internet while complying with industry, government, and regulatory requirements to protect confidential information. Sigaba provides secure message management solutions, including email, instant messaging, and document delivery for the enterprise market. Sigaba Secure Email, Sigaba Secure Statements, and Sigaba Secure Instant Messaging meet the most demanding regulatory requirements, such as Gramm-Leach-Bliley, HIPAA, and SEC, while speeding time to cash and enhancing customer satisfaction. Sigaba's customers' focus includes financial services, government, and healthcare. The company is a member of the Liberty Alliance and a contributing member to the OASIS standards body and is instrumental in making federated authentication a reality for government and financial institutions. Sigaba's future direction is to introduce integrated solutions for application-specific secure message management as it enhances content filtering and management capabilities.

In January of 2005, Sigaba joined the platform partner alliance with IronPort Systems, the market share leader in email security. The IronPort platform partner alliance consists of market-leading antispam, antivirus, encryption, digital rights management, and archiving vendors. The alliance with Ironport will allow Sigaba to strengthen its offerings for companies working to ensure regulatory compliance.

St. Bernard Software

Overview

St. Bernard Software, an Internet filtering company, was founded in 1995 and is headquartered in San Diego, California. It has a global presence, with offices across the United States and Europe.

Secure Content Management Products

St Bernard offers the following SCM products.

- ☒ iPrism is a hardware appliance that monitors, filters, and reports on inappropriate Internet access within businesses, government agencies, and educational institutions.

- ☒ ePrism is an email filtering appliance that delivers a combination of email security, spam protection, and antivirus and content control in an easy-to-use, high-performance appliance.

- ☒ SpyEXPERT allows the removal of spyware and other unwanted agents without damaging legitimate files and applications. It allows the removal of spyware from a central management console and protects mission-critical applications and data.

Strategic Direction

On August 2, 2005, St. Bernard released iPrism 4.0, the latest version of its Internet filtering appliance. iPrism offers enhanced Internet filtering by defending against threats associated with spyware, phishing, instant messaging, and P2P. The company also released the updated ePrism M500, which offers protection from spam and email-borne malicious code. Its multilayer architecture is powered by eGuard, the company's 100% human-reviewed database of spam profiles.

St. Bernard recently introduced SpyEXPERT, the first standalone antispyware software solution specifically designed to meet the needs of small to medium-sized businesses. The addition of SpyEXPERT enhances the company's mission to provide organizations with a complete strategy for spyware protection.

These additions to St. Bernard's existing core product line reaffirm the company's commitment to providing strong network security solutions to organizations.

Vericept

Overview

Based in Denver, Colorado, Vericept Corp. was founded in 1999 and is privately held. Key investors in Vericept include Sigma Partners, Sequel Venture Partners, and William Blair.

Secure Content Management Products

Vericept offers the following SCM products:

- ☒ Vericept's Information Privacy and Compliance Manager addresses the needs of C-level executives as well as compliance, privacy, and corporate governance officers charged with providing information security to company confidential data and protecting the confidentiality of its customers regardless of industry.

- Vericept's Acceptable Use Manager enables organizations to intelligently monitor for infractions against their acceptable use policies and is available for either enterprises or educational institutions. Vericept Filter leverages the URL database from Secure Computing to create a powerful filter to use in combination with content monitoring that protects entire networks and all forms of Internet communications from network misuse and information security breaches.

- Vericept's Preventive Security Manager addresses significant and previously undetectable voids in traditional security frameworks such as enabling network security professionals to stop malicious activity before it happens and notifying when an attack is under way.

- Vericept's Stored Data Analyzer was developed leveraging Vericept's patented Linguistic Engine to analyze and examine stored data.

Strategic Direction

Vericept enables companies to manage financial, compliance, reputation, and productivity risk by analyzing all inbound and outbound Internet traffic for any activity falling outside of a company's internal information controls and acceptable use. Vericept identifies Internet activity placing the company at risk, such as the unauthorized release of private customer information; the leaking of confidential M&A plans; the premature posting of company earnings reports; employees and contractors constantly surfing pornography, shopping, or gambling; and employees using the company network to plan violent acts and network attacks.

In June of 2005, Vericept announced its plans to acquire Black White Box, a leading provider in delivering control and management of endpoint devices. Black White Box's solutions will provide Vericept with the ability to deliver content-based security to endpoint devices, such as laptops, workstations, and USB drives. Customers will now have the ability to manage data in motion as well as data at rest on the network and on end-user devices, to help prevent inappropriate downloading or sharing of information. This protection can extend to mobile devices such as laptops, USB thumb drives, iPods used as hard drives, CD burners, and more. The combination of technologies will also provide a centralized policy management console that will integrate with Vericept's Adaptive Policy Management system.

Vericept's enterprise risk management solutions, combined with services and support, are focused on providing the tools to those responsible for maintaining information security of corporate data.

Cloudmark

Overview

Cloudmark is a private company headquartered in San Francisco, California. The company is a funded software start-up created by veteran entrepreneurs Keen, Napster, Inktomi, Sun, Microsoft, and Netscape.

Secure Content Management Products

Cloudmark offers the following SCM products.

- Cloudmark Immunity, the immune system for email, was developed to help the enterprise attain 100% accuracy and zero false positives through genetic mapping, nD technology, perfect memory, and adaptive learning. Immunity automatically learns the preferences of the enterprise and its employees.

- Cloudmark Authority prevents spam from entering networks. Authority is focused on large businesses, OEM partners, service providers, and carriers.

- Cloudmark Exchange Edition, the maintenance-free, server-side antispam solution for small and medium-sized businesses, leverages the power of the SpamNet community.

- Cloudmark SpamNet was developed specifically for individuals and small businesses seeking instant protection from spam at home or their office

- Cloudmark SafetyBar for Internet Explorer now extends to the browser to protect online users from phishing attacks, identity theft, viruses, and spyware. SafetyBar for Internet Explorer provides consumer and corporate users with a Web site rating so they know when linking to a page whether its "good" or "unsafe" based on real-time feedback from the Cloudmark community. The Web site rating helps users gauge a level of trust before providing personal or confidential information that may put them at risk for identity theft, phishing attacks, or other threats. In addition, enterprises are given real-time updates to provide another layer of protection against Web-based threats.

- Cloudmark Phishing Intelligence Center is a comprehensive set of real-time intelligence derived from data provided by the Cloudmark community and Cloudmark's proprietary forensic analyses that alert banks and financial institutions of the latest phishing attacks and their rate of propagation. The data and analysis are used for actions such as to alert its customers and take action before damage is done, investigate attacks, and prosecute fraudsters. By allowing banks to do better risk management for such attacks, Cloudmark helps facilitate a cost savings for the banks that is in the millions of dollars while restoring trust in online banking and the institution's brand.

- Cloudmark AntiPhishing Reputation Service will be offered as an integrated component of Cloudmark's gateway solutions and sold separately to service providers and OEMs to provide widespread protection from phishing email attacks and phishing Web sites.

Strategic Direction

Cloudmark is a provider of real-time anti--messaging abuse security solutions. It recently announced Cloudmark SafetyBar, Phishing Intelligence Center, and AntiPhishing Reputation Service. SafetyBar's Web site rating helps users gauge a level of trust before providing personal or confidential information that may put them at risk for identity theft, phishing attacks, or other threats. In addition, enterprises are given real-time updates to provide another layer of protection against Web-based threats.

The Cloudmark Phishing Intelligence Center is a comprehensive set of real-time intelligence that alerts banks and financial institutions of the latest phishing attacks and their rate of propagation. The data and analysis are used to alert customers and take action before damage is done, investigate attacks, and prosecute fraudsters.

These gateway solutions enhance Cloudmark's fraud services and protect online users from identity theft, phishing attacks, viruses, and spyware. The use of Cloudmark's existing technology and infrastructure puts them in a position to prevent both Web- and email-based threats.

Proofpoint

Overview

Proofpoint, founded in June 2002, is a messaging security company headquartered in Cupertino, California.

Secure Content Management Products

Proofpoint offers the following SCM products:

- The Proofpoint Protection Server is a message protection software platform (for Linux and SunOS systems) that helps organizations stop spam, protect against email viruses, ensure that outbound messages comply with both corporate policies and external regulations, and prevent leaks of confidential information via email and other network protocols. Proofpoint's solutions run at the enterprise gateway and employ patent-pending Proofpoint MLX machine learning technology to accurately identify incoming spam messages, analyze the contents of outbound messages for regulatory compliance violations and the presence of confidential information, and to identify malicious network-level connections.

- The Proofpoint Messaging Security Gateway offers the same features as the Proofpoint Protection Server software in a hardened, easy-to-deploy appliance. Both enterprise versions (the P-Series appliance) and SME versions (the X-Series appliance) are offered in a variety of different models.

- Both software and appliance versions can be configured with a variety of modular defenses including spam detection, virus protection, content compliance (for policy enforcement), digital asset security (for protecting intellectual property), regulatory compliance (for HIPAA, GLBA and Sarb-Ox compliance) and secure messaging (encryption) modules.

- The Proofpoint Network Content Sentry is a separate appliance that monitors all outbound network traffic in real time, allowing Proofpoint policies to be applied to additional message streams including Web-based email, blog and message board postings, and other HTTP- or FTP-based activity.

Strategic Direction

Proofpoint is a messaging infrastructure company that is pioneering enterprise software solutions uniquely matched to the needs of the large corporate customer. Proofpoint's solutions, offered as both software and as a hardware appliance, are designed to mitigate both inbound and outbound email-borne threats — helping organizations stop spam, protect against email viruses, ensure that outbound messages comply with both corporate policies and external regulations and prevent leaks of confidential information via email and other network protocols. Both of these are based on the same MLX machine learning technology and can be configured with a wide variety of inbound and outbound protection modules. A new series of Proofpoint Messaging Security Gateway appliances designed specifically to meet the needs of small and medium-sized enterprises was announced in June of 2005. The Proofpoint Messaging Security Gateway X-Series appliance provides antispam, antivirus, and email firewall capabilities and protects SMEs from message-borne threats at the gateway. In August 2005, Proofpoint became the first enterprise messaging security vendor to extend its email content security and policy enforcement capabilities to Web email, message board postings, and FTP with the introduction of the Proofpoint Network Content Sentry appliance.

The Proofpoint family of products is built on a programmable platform that is extensible, scalable, and manageable through a common set of interfaces and deployed within the network of corporate enterprises.

Proofpoint is also focused on reducing the administrative burden of managing messaging security solutions. By providing centralized administration for all messaging protection applications, Proofpoint significantly reduces the ongoing operational costs of large, complex messaging deployments.

Internet Security Systems

Overview

Internet Security Systems (ISS), an established world leader in Internet security since 1994, is headquartered in Atlanta, Georgia, and maintains more than 39 offices in 26 countries worldwide. On January 14, 2004, ISS acquired Cobion AG, a content security pioneer. ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 12,000 customers worldwide.

Secure Content Management Products

ISS offers the following SCM products:

- Proventia Web Filter blocks and helps improve productivity and enforce Internet usage policies. Proventia Web Filter has more than 20 million catalogued Web sites and is constantly and automatically updated with 100,000 new and updated Web pages added to the database each day.

- Proventia Mail Filter is a comprehensive antispam and mail filtering solution. Proventia monitors the content of email traffic, eliminating spam and blocking undesirable or illegal content. Proventia Mail Filter avoids blocking legitimate email using a 10-step analysis process to ensure accurate spam detection.

Strategic Direction

Cobion's OrangeBox Web and OrangeBox Mail are now part of Internet Security Systems' Proventia line of enterprise security products for protection from the desktop to the datacenter against a full spectrum of online threats. The Cobion acquisition enables ISS to deliver best-of-breed content security either as a standalone product or via the Proventia all-in-one protection appliance, fulfilling ISS' security convergence strategy announced last October. Proventia incorporates advanced intrusion prevention, firewall, VPN, vulnerability scanning, and antivirus, as well as mail security and Web filtering.

ISS plans to introduce Proventia Mail Filter and Proventia Web Filter in standalone appliance form factors in the near future.

eSoft

Overview

Founded in 1984 and based in Broomfield, Colorado, eSoft strives to provide small and medium-sized enterprises with sophisticated, multitier network security solutions.

Secure Content Management Products

eSoft's InstaGate Secure Content Management (InstaGate SCM) solution combines preintegrated, policy-based Internet security tools that manage email content, Web content, virus protection, and more — all on a single platform. eSoft's ThreatWall is a combination of hardware and software that offers protection from security threats with a high-speed Intel processor and dual hot-swappable mirrored (RAID1) drives to ensure constant network protection. Individual security SoftPaks may be downloaded as needed ThreatWall supports SpamFilter, Gateway Anti-Virus, Desktop Anti-Virus, SiteFilter, and Email Server SoftPaks.

Strategic Direction

eSoft focuses on providing small and medium-sized enterprises with the sophisticated, multitier network security solutions available in the simplest way possible. The company delivers to more than 12,000 customers next-generation Internet security appliances that integrate all of the security tools and services organizations need on one extensible platform, reducing the time and complexity required to mount an effective defense enterprisewide. With services such as antivirus and spam, Web site, and content filtering, eSoft provides solutions that ensure a high degree of customization and scalability while reducing the costs and complexity typically associated with maintaining an effective network security system.

eSoft's ThreatWall brings enterprise-quality reliable threat protection to small and medium-sized businesses at an affordable cost. ThreatWall stops spam and viruses before they enter networks and prevents inappropriate Web and email use.

eSoft's InstaGate SCM also offers multiple deployment options, making it easy to integrate into existing networks, and can be implemented in conjunction with other firewalls and mail servers without reconfiguring an existing network. This simple integration protects the investment a company has made in its current network security solution while at the same time providing best-of-breed email and Web content filtering for a complete, multilayered defense

FaceTime Communications

Overview

FaceTime Communications was founded in 1998 and is headquartered in Foster City, California. It is a provider of security solutions for the management and control of greynet applications and has more than 500 customers worldwide.

FaceTime offers the following SCM products:

☑ FaceTime Enterprise Edition manages, secures, and controls IM, P2P, spyware, and other greynet applications. It provides user policy management, message hygiene, archiving for compliance, blocking of unauthorized usage, and network protection against sophisticated workarounds. FaceTime Enterprise Edition can also be configured to prevent spyware infection and offer targeted remediation of spyware-infected desktops.

☑ FaceTime RTGuardian (RTG) is a perimeter security solution for preventing spyware and greynet applications and securing unauthorized IM and P2P usage. Designed for deployment in the internal LAN as well as the corporate DMZ, RTG 3.0 acts as a security gateway that provides protection from the spread of spyware and application vulnerabilities, as well as the ability to block unauthorized connections and file transfers and obtain rich IM and P2P usage statistics.

☑ FaceTime IMAuditor offers regulation and security of instant messaging and ensures IM communications comply with corporate policy and government regulations.

☑ FaceTime RTShield is an appliance that allows compliance with regulations regarding electronic messaging retention without an extensive IT infrastructure. It is based on a secure integrated appliance and may log, audit, and archive IM and email traffic with virtually no latency.

Strategic Direction

FaceTime is a provider of products that protect against security threats in instant messaging and peer-to-peer traffic. FaceTime recently introduced IMPact Index, which assesses "point-in-time" risks posed by viruses, worms, and other malware propagating through greynet applications.

In June 2005, FaceTime acquired of XBlock Systems LLC, maker of the X Cleaner antispyware software. X Cleaner contains spyware scanning, inoculation, and removal capabilities, in addition to privacy protection features like file shredding and encryption tools. The technology enhances detection of unsanctioned programs that evade existing security products and undermine enterprise security. Researchers obtained in the acquisition bolster FaceTime Security Labs by providing spyware knowledge and expertise to compliment the company's existing IM and P2P researchers.

FaceTime is broadening its focus to "greynets," which encompasses adware, spyware, and legitimate applications like IM, Web conferencing, and peer-to-peer file sharing. The XBlock acquisition will allow FaceTime to spot adware and spyware installations on enterprise networks that its products protect, in addition to IM and P2P applications. Facetime is a key provider of security solutions for the management and control of greynet applications such as adware/spyware, instant messaging, Web email, P2P file sharing, Web conferencing, and instant voice

IMlogic

Overview

IMlogic is a global provider of instant messaging management and security software. Organizations of all sizes depend on IMlogic solutions to manage, control, and secure IM usage, while satisfying compliance requirements associated with real-time electronic communications. Headquartered in Waltham, Massachusetts, IMlogic distributes its products in 26 countries and manages over one million deployed seats worldwide.

Secure Content Management Products

IMlogic offers the following SCM products:

☒ IMlogic IM Manager controls and secures the use of public and enterprise IM for real-time communication while ensuring compliance with legal and corporate governance policies. It manages and archives all IM traffic, provides IM hygiene and antivirus, and offers certified support for public and enterprise IM networks.

☒ IMlogic Real-Time Threat Protection System protects enterprise networks from zero-day IM attacks using predictive threat detection to automatically quarantine and block IM virus and worm outbreaks before they occur. This product integrates with IMlogic IM Manager and the IMlogic Threat Center, the global clearinghouse for IM threat activity.

Strategic Direction

IMlogic is a key provider of enterpriseclass solutions for secure instant messaging management to businesses of all sizes. IMlogic enables these organizations to leverage IM as a business-critical tool for real-time communication and collaboration while safeguarding IM usage.

IMlogic's flagship product, IMlogic IM Manager manages, secures, logs, and archives all IM traffic with certified support for public and enterprise IM networks, including AOL, MSN, Yahoo!, ICQ, IBM Lotus Instant Messaging, Microsoft Office Live Communications Server 2003/2005, Jabber, Reuters, and multiple XMPP (Google Talk) and SIP/SIMPLE platforms. Through a single solution for instant messaging management, security, and compliance, IMlogic IM Manager manages and controls instant messaging. The product secures corporate networks against IM security threats such as IM viruses, malware, IM spam, and intellectual property loss and satisfies regulatory compliance and corporate governance standards for logging, archiving, and auditing IM conversations.

The company operates the IMlogic Threat Center, a global clearinghouse for all IM and P2P threat activity. Launched in December 2004 with the support of Internet security leaders Symantec and McAfee, and global instant messaging leaders America Online, Microsoft, and Yahoo!, the IMlogic Threat Center provides rapid response and guidance for protection against newly-detected threats. The IMlogic Threat Center is focused on providing early warning and remediation for IM-based attacks to both enterprise and consumer IM users.

IMlogic's close technology partnerships with email compliance and security vendors such as EMC, Symantec/Veritas, and McAfee, enable companies to integrate IM management and security with existing email infrastructure. In June 2005, the company signed an OEM agreement with Postini, a managed services leader for email perimeter security, to deploy an integrated email and IM management service to Postini's more than 5,000 customers and over seven million seats.

IMlogic also partners with the major IM network providers to drive its product roadmap and to further enhance the enterpriseclass capabilities of the underlying IM services. In 2002, Microsoft licensed logging and archiving technology from IMlogic to embed into Microsoft's next-generation enterprise real-time communication solutions, the Microsoft Live Communications Server. In 2004, AOL chose to migrate customers of its AIM Enterprise Gateway solution to IMlogic IM Manager when AOL shifted focus from enterprise software to AIM network services.

Mail-Filters Inc.

Overview

Founded in 2001, Mail-Filters is located in San Mateo, California, with additional offices in Portland, Oregon, and London, England. Mail-Filters products are used to protect businesses and consumers from spam and "spim" (instant message spam).

Secure Content Management Products

Mail-Filters offers the following SCM products:

☒ SpamCure is a server software email gateway solution that allows the quarantine and deletion of spam. The Mail-Filters Bullet Signatures Database enables the detection of spammers and the messages they send. The Mail-Filters STAR Engine detects spammer tricks, allowing it to catch new types of spam, such as embedded content, HTML, and foreign language spam.

☒ SpamRepellent is a fully managed antispam service that allows administrators and users to customize their filters. SpamRepellent filters email at Mail-Filters' datacenters.

☒ StarEngine SDK allows quick and easy integration of antispam technology into OEM software or appliance solutions.

Strategic Direction

Mail-Filters launched SpamCure in June 2002. SpamCure is a combination of software and service solution, using SpamRepellent technology but designed to filter spam at the customer's premises rather than at Mail-Filters' datacenters.

Mail-Filters' OEM solution allows companies to incorporate the Mail-Filters technology to provide an antispam solution. Mail-Filters has focused most of its attention toward providing its technology through OEM partners. Its client base amounts to 30,000 enterprise customers, and Mail-Filters is deployed in more than 100 countries and supports more than 30 languages.

With its international presence, Mail-Filters opened its first international office in London, England, in late-2004. In early 2005, Mail-Filters opened an office in Tokyo, Japan.

MailFrontier

Overview

Founded in 2002, MailFrontier is an email security company funded by New Enterprise Associates (NEA), Draper Fisher Jurvetson (DFJ), and Menlo Ventures.

Secure Content Management Products

MailFrontier offers the following SCM products:

☑ MailFrontier Gateway Server provides email protection by blocking 98% of spam, fighting virus outbreaks, eliminating phishing fraud, stopping DHA/DOS attacks, defending against zombie machines, and detecting policy violations.

☑ MailFrontier Gateway Appliance is a preconfigured, prehardened solution that offers control of the MailFrontier Gateway email security solution with immediate deployment.

☑ MailFrontier Desktop protects users from spam and fraud with techniques that can be trained to match a user's email security preferences. MailFrontier Desktop is designed for ease of use with multiple email accounts.

Strategic Direction

MailFrontier is an email security company that delivers protection from spam, viruses, phishing, and every other form of inbound and outbound email threat. The MailFrontier Gateway Product Suite has adapted to the ever-changing security needs of the end user. It includes MailFrontier Desktop, which screens out nonsupported foreign language character sets that are a sign of spam. The small business edition of the MailFrontier Gateway Server combines protection with easy administration for organizations of up to 100 users. MailFrontier is currently used by approximately 800 companies worldwide.

Mirapoint Inc.

Overview

Mirapoint, founded in 1997, offers messaging and security solutions through purpose-built appliances designed to protect data networks. Mirapoint has 180 employees and is headquartered in Sunnyvale, California.

Secure Content Management Products

Mirapoint offers the following SCM products:

- Mirapoint's RazorGate is a security appliance that prevents email-specific attacks and includes antispam, antivirus, and SMTP connection management features.
- Mirapoint Message Server is an email server designed for small, medium-sized, and large businesses. It provides desktop email as well as Web and wireless access. It also features integrated technology to block spam, viruses, and hacker attacks, in addition to a portfolio of collaborative services such as group calendaring.

Strategic Direction

Mirapoint is focused on the continued sales of Message Server to key service provider, education, government, and enterprise customers. Mirapoint's Message Server is an alternative to more traditional enterprise messaging products and is a versatile solution for a variety of employee segments. Message Server offers Webmail and collaboration features, as well as email, group calendaring, and address book functionality. Mirapoint's RazorGate offers a standalone email security appliance, which complements existing email servers (both Mirapoint and non-Mirapoint). Mirapoint continues to focus on building solutions that can prevent and filter out email threats

Network Appliance Inc.

Overview

Network Appliance (NetApp) is a vendor of network-attached storage systems designed for medium-sized to large enterprises. Founded on 1992, Network Appliance has 3,900 employees, 89 worldwide offices, and 60,000 worldwide installations.

Secure Content Management Products

NetApp NetCache is a scalable suite of Web delivery and security appliances. NetCache appliances are deployed across the entire network, from the primary datacenter to remote points of presence (POPs) and local offices worldwide. NetCache offers customers granular access controls, URL filtering, antivirus and spyware protection, bandwidth management, and other services to minimize the management complexity and increase the security of Internet access.

Strategic Direction

In 2004, NetApp was a key vendor in the secure content application and delivery market worldwide. It serves a diversified customer base that includes large enterprises and service providers with tools that simplify data management.

The value of the NetCache product line is displayed by its delivery of information for enterprises — providing security, accelerated information access, cost savings, and reliability. In the past year, NetApp solutions have offered a broader range of features, increased storage capacity, and value-added services of NetCache appliances. NetApp is currently focused on providing more solutions to simplify Internet security and content delivery.

Entrust Inc.

Overview

Headquartered in Addiston, Texas, Entrust is a global provider of security software.

Secure Content Management Products

Entrust offers the following SCM products:

☒ Entrust Secure Messaging Solution offers real-time corporate and regulatory policy enforcement, including automatic protection of sensitive information at the boundary. It is an integrated suite of components that provides automatic content scanning of inbound and outbound email messages, centralized policy enforcement, and boundary-based email encryption. The specific product components of the Secure Messaging Solution include:

- □ Entrust Entelligence Messaging Server is a server-based security gateway that makes it easier to communicate securely with external partners and customers. Messaging Server transparently manages security functions and enforces corporate secure email policies and enables "end-to-end" and "boundary-only" encryption. Messaging Server supports multiple messaging platforms and delivers methods and protocols to enable flexible and secure communications outside of the organization.

- □ Entrust Entelligence WebMail Center is an optional add-on to Messaging Server that allows secure Web-based communications for those recipients without certificates or S/MIME capabilities. Through a simple Web browser and a Web-based email account, recipients are able to retrieve, read, and reply to any secure emails delivered through the Entrust Entelligence WebMail Center.

- □ Entrust Entelligence Compliance Server is an outbound content compliance solution that uses highly sophisticated content analysis tools to automatically analyze and categorize email messages and document content based on the contextual meaning, not simply predefined word lists.

- Entrust Entelligence Desktop Manager and E-Mail Plug-in provides "government strength" (FIPS, Common Criteria, NIST, and PKITS certified) email security down to the desktop environment, protecting email messages while in transit and while stored on the desktop.

Strategic Direction

Entrust's software and services are deployed to ensure the privacy of electronic communications and transactions across corporate networks and the Internet, addressing functions such as identification, verification, privacy, and security. Entrust's software is used to authenticate users via smart cards, passwords, digital certificates, biometric devices, and all-new "grid authenticaiton" with Entrust IdentityGuard controlling access to information in email, databases, Web pages, and business applications. The company also offers services such as consulting, deployment, and managed security services.

In mid-2004, Entrust acquired AmikaNow! Corporation's advanced content scanning, analysis, and compliance technology. The Entrust Entelligence Compliance Server is designed to automatically analyze and categorize email messages and document content based on the contextual meaning. Policies can be customized to suit the corporate environment and be automatically enforced at the boundary to help customers reduce business risk and help in their compliance with privacy and securities laws including HIPAA, GLB, PIPEDA, and various SEC regulations. By adding boundary email and data security capabilities with its traditional end-to-end encryption and digital signatures functionality, Entrust is focused on becoming the leader in outbound content compliance, delivering comprehensive, single-source secure data and secure messaging solutions for enterprises and governments worldwide.

IronPoint Technology

Overview

IronPoint was founded 1995 and is headquartered in Vancouver, British Columbia, Canada. IronPoint provides more than 200 customers and 75,000 end users with a comprehensive content management product suite to communicate clearly through the Web and across the enterprise.

Secure Content Management Products

IronPoint Enterprise Content Manager Suite is a content management product that enables organizations to transform their Web properties into strategic assets by extending content management capabilities beyond the Web team while ensuring compliance. It allows managers, department leads, and others to administer their own content and/or content sites using simple, predefined templates. Templates allow business users to create and publish new content based on preexisting models and layouts, which ensure that content experts focus on content and Web designers can focus on design.

Strategic Direction

IronPoint provides Web-based software that allows organizations to create, manage, and publish the content that drives business processes and collaboration. IronPoint's Enterprise Content Manager Suite is an extensible and scalable solution for Web content and document management that is used by hundreds of organizations in North America. IronPoint facilitates collaborative creation and transforms, manages, delivers, and archives the knowledge that drives business operations, from documents, records, and systems to Web pages and rich media. Based on a single framework, IronPoint has developed specific solutions for the government, education, community, and library markets.

Kaspersky Lab

Overview

Founded in 1997, Kaspersky Lab is a developer of secure content management solutions that protect against viruses, spyware, spam, and hacker attacks. Kaspersky Lab is headquartered in Moscow, Russia, with regional offices in the United States, the United Kingdom, France, Germany, the Netherlands, Poland, Japan, and China. It maintains a large partner network comprising more than 500 companies globally and has OEM partnerships with more than 50 well-known security solutions providers.

Secure Content Management Products

Kaspersky offers the following SCM products:

- Kaspersky Business Optimal family of products is designed to provide protection against malicious code at all points of entry into enterprise information systems from firewalls, gateways, and mail servers to fileservers and workstations. These products offer extensive multiplatform protection across Windows, Linux, and Unix environments.

- Kaspersky's Administration Kit offers a management console with a set of system tools for centralized administration of installation, configuration, and monitoring from any node in the network.

- Kaspersky Anti-Spam Enterprise Edition for mail servers provides robust spam filtration of incoming mail transmitted by SMTP and attachments using linguistic heuristics, based on term databases and fuzzy mathematics.

- Kaspersky also offers a line of personal security products for mobile workers and for personal- and SOHO users. These provide protection against viruses, spyware, worms, trojans, spam, hackers, and adware.

Strategic Direction

With the rise of Internet crime for identity theft, phishing, denial of services, and fraud, Kaspersky Lab believes that proactive and rapid response is a critical requirement for protecting corporate information. Through its information security lab based in Moscow, The Russian Federation, Kaspersky offers one of the highest detection rates in the industry, creates protective antivirus signatures within twenty minutes of entering its lab, and offers the industry's first automated hourly antivirus updating.

Currently, Kaspersky OEMs its antivirus engine to more than 50 information security hardware and software providers — companies such as Aladdin, Astaro, Borderware, F-Secure, MailFrontier, Sybari, and others. Through the company's direct operations and its OEM partnerships, Kaspersky protects more than 75 million users worldwide.

Microsoft Corp.

Overview

Microsoft is the world's largest software company and provides a variety of products and services, including its Windows operating systems and Office software suite. It was founded in 1975 and is headquartered in Redmond, Washington. In the area of security, Microsoft is expanding its reach to provide solutions to commercial and consumer users.

Secure Content Management Products

Microsoft offers the following SCM products:

- Microsoft Windows Anti-Spyware is a security technology that helps protect Windows users from spyware and other potentially unwanted software. It reduces negative effects caused by spyware, including slow PC performance, annoying pop-up ads, unwanted changes to Internet settings, and unauthorized use of private information.

- Microsoft acquired Sybari Software Inc. in June 2005. This acquisition was primarily meant to beef up Microsoft's security offering in the enterprise market. Sybari offers antivirus, general protection, and security attributes used by corporate networks that have deployed Microsoft Exchange or Lotus Notes platforms.

- To further expand its security offering to the enterprise market, Microsoft acquired in July 2005 venture-backed FrontBridge Technologies, a provider of email security and antispam technology, for an undisclosed investment. FrontBridge Technologies provides secure email and messaging software used to protect business networks and corporate email systems.

- In the consumer and small business space, Microsoft announced in May 2005 plans to provide antivirus and other security protection to consumers under a program called Windows OneCare. The program will be based on a subscription service that will help Microsoft compete against the well-entrenched Computer Associates, McAfee, and Symantec. Windows OneCare will provide automated protection, maintenance, and performance tuning as an all-in-one package for Windows-based PCs.

Strategic Direction

With its platforms facing mounting virus attacks and security threats, Microsoft is responding by investing in technologies that will enable more protection for its operating systems and applications such as Outlook, Messenger, and other tools with Internet access capability. Microsoft investments in security areas come in two forms. The first is through the acquisition of existing companies such as Sybari Software and

FrontBridge Technologies with the aim of penetrating the commercial market. The second strategy being adopted by Microsoft is to build security tools that will be integrated into its existing OSs and offerings with the recently announced Windows OneCare program. IDC believes these steps are not only necessary for Microsoft but they will also position the company as a key player in the secure content management market along with long-established vendors such as Computer Associates, McAfee, and Symantec.

Panda Software

Overview

Panda Software develops antivirus and intrusion prevention software to protect home users, small and midsized businesses, and large corporations. A private company founded in 1990 and headquartered in Bilbao, Spain, Panda Software sells its products and services to consumers and businesses in more than 200 countries around the world.

Secure Content Management Products

Panda Software offers the following SCM products:

- Panda Titanium Antivirus prevents attacks from all types of viruses, worms, and Trojans. It automatically detects and blocks unknown viruses and intruders and offers antispyware, antidialer, antiphishing, and firewall technology against hackers. Titanium Antivirus employs a heuristic engine integrating signature correlation techniques, analyzing typical malware traits and code that are active in critical PC entry points, email, and instant messaging.

- Panda Platinum Internet Security offers daily virus-pattern file updates, extensive configurability, and an easy-to-use interface. For personal or small and even medium-sized businesses, Platinum Internet Security allows scanning of Microsoft or Novell network drives. Systems can be configured to send email alerts when an infection occurs. They can also broadcast alert messages to other Panda users on Windows NT/2000/XP Pro systems on the same network or domain.

Strategic Direction

Panda Software's centrally managed security solutions protect servers, gateways, and endpoints, ensuring an effective and simple-to-use line of defense against Internet threats for enterprises, small and medium-sized businesses, and home users. Panda's solutions are backed by an expert team of technical support service professionals.

Panda is a fast-growing company, with sales increasing by 55% in 2004. Panda seeks to continue to consolidate its presence in the antivirus and intrusion prevention software market by continuing to offer integrated solutions. Panda Research heads the company's efforts to analyze security threats and offers around-the-clock coverage and security alerts. Panda will continue to focus on small to medium-sized businesses' security needs, seeking to repeat its strong sales performance of last year.

Tenebril Inc.

Overview

Tenebril is a privately held company founded in 1988 with offices in Boston, Massachusetts, and Silicon Valley, California. Tenebril is a leading security and privacy technology company.

Secure Content Management Products

Tenebril offers the following SCM products:

- Tenebril SpyCatcher enterprise provides spyware protection through real-time monitoring, a unique reinstallation shield, and automatic updates to its spyware database. SpyCather uses a Spyware Profiling Engine, which goes beyond traditional signature and behavior analysis technologies to add a third layer of analysis — contextual analysis. This three-pronged approach to blocking and removing spyware allows SpyCatcher proactive protection against new strains of spyware, such as hypermutating spyware, as well as against known spyware strains. SpyCatcher provides central management capabilities using an anywhere, anytime Web-based management console. Tenebril's consumer product line up includes SpyCatcher 2006, which also features profiling technology, the Spyware Profiling Engine, as well as a new easier-to-use UI, a suspicious file wizard, antiphishing technology, and a DeepDefense technology, which prevents spyware, malware, and rootkits from installing and causing harm.
- SpyCatcher Express includes all the spyware protective features of SpyCatcher — the profiling and DeepDefense technologies, new UI, and suspicious file wizard — in a free product availabile on Tenebril's Web site.
- Tenebril GhostSurf provides an anonymous Internet connection for Web invisibility. It works with all Web browsers and also supports instant messengers, newsgroups feeds, and popular chat programs. GhostSurf also erases Web history, cache, clipboard, and cookies.

Strategic Direction

Tenebril GhostSurf 2005 Platinum, a Web invisibility software, debuted in September. In addition to its IP address masking, the application encrypts Internet connections and erases Web histories, temporary files, cookies, and any other traces of Web use in compliance with Department of Defense standards.

Also included in GhostSurf 2005 Platinum is a battery of Tenebril Internet security products, including SpyCatcher, an antispyware defense; AdArmor, a tool to deter pop-up ads; and Personal Data Vault , an encrypted and password-protected "safe deposit box" for all forms of private digital information.

The release of Tenebril SpyCatcher 3.5 on January 5, 2005, has strengthened Tenebril's presence in the antispyware market. Its new features include an upgraded detection engine with more efficient search algorithms, faster scan times, and antiphishing capabilities. SpyCatcher 3.5 monitors every part of the user's PC, including memory, registry, network drives, hard disks, and removable or optical drives, ensuring complete protection.Tenebril's new offerings advance its presence in the security and privacy technology market. Tenebril focuses on the Fortune 1000 enterprise market as well as the consumer and small business markets.

Tablus Inc.

Overview

Tablus Inc is a leading provider of content protection solutions. Founded in 2002, Tablus delivers complete end-to-end content protection solutions to prevent unauthorized or unintended dissemination of confidential information. By preventing such disclosures, Tablus helps organizations reduce legal and financial risk, preserve brand equity and competitive advantage, and prove regulatory compliance. Tablus is privately held, with funding from Menlo Ventures in February 2004.

Secure Content Management Products

Tablus offers the following SCM products:

- The Tablus Content Alarm solution suite includes Content Alarm NW for the network and Content Alarm DT for the desktop. The Content Alarm solutions may be deployed separately. Together, the products provide a complete content protection solution that offers central policy administration and enforcement with automatic "information DNA" updates to ensure confidential information is protected at all points in its life cycle.

- Content Alarm NW protects confidential information such as customer data and intellectual property from disclosure. It continuously monitors, accurately detects and blocks or quarantines the outbound transmission of confidential information via the network, supporting most network communications, not just email.

- Content Alarm DT provides visibility and control over confidential information on the desktop, enabling organizations to audit actions, monitor threshold behaviors for anomalies, enforce policies, and ultimately stop the misuse of data before it happens.

Strategic Direction

Tablus Inc. provides a comprehensive content protection solution for detecting and preventing the disclosure of confidential and privacy-related information. This includes personally identifiable information, customer information, financial statements, design specifications, and source code.

The Tablus Content Alarm Solution suite protects against the loss of information across the network and on the desktop. This unique approach ensures that customers can protect their most valuable information by blocking or quarantining email transmissions or preventing that information from being written out to removable storage like USB flash drives and CD ROMs. Tablus' solution for protecting confidential information enables organizations to comply with privacy regulations, reduce legal and financial risk, enhance customer trust and confidence, and safeguard trade secrets and competitive advantages.

SonicWALL Inc.

Overview

Founded in 1991, SonicWALL Inc. is a leading provider of integrated network security, mobility, and productivity solutions. Today, it is the worldwide leader in unified threat management appliances according to IDC's latest *Quarterly Worldwide Tracker Report*, offering content filtering, antivirus, intrusion prevention, and antispyware across its entire range of latest-generation firewalls and appliance-based products

SonicWALL works with over 10,000 channel partners to deliver its deep packet inspection-based appliances and software solutions to small, medium-sized, and distributed networks in the enterprise, ecommerce, education, healthcare, retail/point-of-sale, and government markets. Over 50,000 SonicWALL units worldwide are managed by SonicWALL's award-winning Global Management System software, and to date more than 680,000 SonicWALL security appliances have shipped to protect millions of users around the globe.

Secure Content Management Products

SonicWALL offers the following SCM products:

☒ SonicWALL Content Security Manager integrates a comprehensive suite of antivirus, antispyware, and content filtering services on a standalone appliance that works behind virtually any manufacturer's firewall. It provides protection from threats such as viruses, worms and trojans, spyware, adware, keyloggers, malicious applications, or phishing schemes and enables users to filter unacceptable or illegal online content. IT administrators can also use the solution to manage bandwidth usage by regulating recreational file-sharing, multimedia streaming, and downloading from peer-to-peer applications as well as nonproductive online surfing, chatting, messaging, and shopping.

☒ SonicWALL Gateway Anti-Virus, Anti-Spyware, and Gateway Intrusion Detection Service delivers intelligent, real-time network security protection against viruses, spyware, worms, trojans, and application exploits. Utilizing a configurable, high-performance deep packet inspection architecture, it secures the network from the core to the perimeter against a comprehensive array of dynamic threats and software vulnerabilities such as buffer overflows, as well as peer-to-peer and instant messenger applications, backdoor exploits, and other malicious code.

☒ SonicWALL Content Filtering Services (CFS) enable businesses and schools to transparently enforce productivity and protection policies and block inappropriate, illegal, or dangerous Web content. Featuring a dynamic rating and caching architecture, SonicWALL CFS Standard and Premium Editions block multiple categories of objectionable Web content, providing the ideal combination of control and flexibility to ensure the highest levels of productivity and protection.

- SonicWALL Complete Anti-Virus and Network Anti-Virus are distributed, gateway-enforced solutions that ensure always-on, always-updated antivirus software for every client or server on the network. SonicWALL has customized McAfee's award-winning Managed VirusScan and Groupshield to provide these highly automated and enforced solutions.

Strategic Direction

SonicWALL is numbered among the leading vendors in SCM appliance revenue for 2004. SonicWALL's SCM technology is designed to maximize network protection, optimize network utilization, and enable precise control over Internet usage, and the company continues to extend its appliance-based solutions to the SCM market.

SonicWALL recently announced the general availability of version 2.0 of their Content Security Manager (CSM) 2100 CF appliance, which combines dynamic threat management with flexible control over Internet usage in an affordable, easy-to-manage solution. With the addition of gateway antivirus and spyware protection, SonicWALL's appliance also becomes a powerful extension to network security, especially in older networks where the existing firewall may not be capable of dealing with dynamic threats. An onboard dynamic rating engine enables users to obtain real-time ratings for new, unrated URLs. This solution works in virtually any network to deliver powerful, scalable threat protection leveraging existing network resources.

SonicWALL will continue to develop integrated SCM technology based on its "value innovation" strategy of taking complex, state-of-the-art networked security and simplifying the implementation in a cost-effective solution that makes its customers feel safe and in control.

LEARN MORE

Related Research

- *North American Security Software 2005–2009 Forecast by Vertical Market* (IDC #33761, August 2005)
- *Microsoft Announces OneCare: Friday the 13th for Consumer Security Vendors?* (IDC #33603, June 2005)
- *Trend Micro Acquires InterMute: Spyware Consolidation Continues* (IDC #33401, May 2005)
- *Worldwide SSL-VPN Appliance 2005–2009 Forecast and 2004 Vendor Shares: Delivering Secure Application Access* (IDC #33142, March 2005)
- *Digital Security Spectrum, 4Q04* (IDC #33094, March 2005)
- *Worldwide Secure Content Management 2005-2009 Forecast: The Emergence of Outbound Content Compliance* (IDC #33076, March 2005)
- *IDC's Software Taxonomy, 2005* (IDC #32884, February 2005)

- *IDC's Enterprise Security Survey, 2004* (IDC #32593, December 2004)
- *Worldwide IT Security Software, Hardware, and Services 2004–2008 Forecast: The Big Picture* (IDC #32557, December 2004)
- *Quantum Cryptography: Where It Stands* (IDC #32517, December 2004)
- *Worldwide Email Usage 2004–2008 Forecast: Spam Today, Other Content Tomorrow* (IDC #31782, August 2004)

Methodology

The IDC software market sizing and forecasts are presented in terms of "packaged software revenue." Packaged software is defined as programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately as software maintenance. Upgrades may be included in the continuing right of use or may be priced separately.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license but *includes* the implicit value of software included in a service that offers software functionality by a different pricing scheme (e.g., the implicit or stated value of software included in an application service provider's [ASP's] or other hosted software arrangement). It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

- **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2004 as of the end of April 2005, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q04–4Q04 in nearly all cases and through 1Q05 in many cases).
- **IDC's *Software Census* interviews.** IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.
- **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.

- **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area models on more than 1,000 worldwide vendors.

- **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC's best estimates based on the above data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Published Under Services: Security Products; Secure Content Management

EXHIBIT 25

SECURE COMPUTING PartnersFirst

Webwasher Hot Sheet

What is Webwasher?

webwasher Webwasher® from Secure Computing® includes appliance- and software-based solutions designed to protect against inbound Web-based threats such as spyware, phishing, viruses, worms, Trojans, and other types of malicious code*. Webwasher is designed to protect against Web-based outbound threats as well, such as confidential data, customer records, intellectual property, and other sensitive information leaving an organization.

Why is Web Gateway Security "hot"?

Compared to other markets showing signs of saturation, such as routers, switches, and caching devices, the Web Gateway Security market is expected to show double-digit growth rates until 2009, as per IDC's March 2006 World SCM Forecast report*. According to a recent study by the CSI institute, 97% of all surveyed businesses had a firewall solution in place (*http://www.gocsi.com/*); while estimates show only 30% (small enterprise) to 70% (large enterprise) have a gateway anti-virus or content security solution for all Web protocols deployed. Out of these, the vast majority is dependant on old-school, signature-based virus scanning engines and are in no way equipped to cope with today's ongoing bombardment of day-zero threats and blended attacks not visible to a traditional firewall or conventional anti-virus engine.

How can my customers evaluate Webwasher?

Testing Webwasher is easy and fun. It installs in minutes and with easy documentation that runs you through the initial setup, the process is a breeze. You and your customers are welcome to test Webwasher by filling in the evaluation form (*www.securecomputing.com/goto/webwasher/eval*). Instructions where to obtain the software and licenses will be emailed shortly there after.

Why sell Webwasher from Secure Computing?

- Webwasher addresses a growing market.
- Great cross-selling opportunity for existing firewall or SmartFilter® customers who want to be "more secure."
- Complementary product to many existing network security solutions; easy to approach customers.
- Great up-sell potential: lead with one product; additional modules provide up-sell potential.
- Excellent margins on initial sale and recurring revenue on subscription renewals.
- Easy to sell - no premium add-ons or complicated product pricing / licensing to confuse customers.
- All-in-one pricing including all updates and 24x7 support.
- Excellent product for writing RFP/RFI "lock-out" specs.
- Wide target audience - caters to the needs of a few hundred users to global deployments and ISPs.
- Excellent product to create interest and penetrate new accounts.

What is Secure Computing's Web Gateway Security solution?

Already a strong player in the European market and market share leader in the Central European region, Webwasher is Secure Computing's Web Gateway Security product line. For more info on the history of Webwasher, please see the Fact Sheet on PartnersFirst.

What does Webwasher do?

Webwasher provides a fully integrated solution for handling of Web, FTP, and even encrypted SSL (HTTPS) traffic as well as the ability to control all leading Peer-to-Peer and Instant Messaging applications. To take control, URL Filter serves as a first line of defense to block unwanted content. Webwasher enables easy blocking of unwanted file types (e.g. block ActiveX on untrusted sites), pop-ups, and advertising, as well as check for digital signatures on any active content.

For the next layer of defense you can choose up to three leading anti-virus engines and the Secure Anti-Malware engine to run simultaneously. Additionally, any piece of active code can be inspected for malicious behavior with Secure Computing's Proactive Security™ solution, available in Webwasher Anti-Malware. To apply the above checks on encrypted content within the HTTPS protocol, the Webwasher SSL Scanner unlocks encrypted traffic for inspection and re-encrypts it afterwards. At the same time, the Webwasher Instant Message filter keeps locks on unsanctioned use of more than a dozen Instant Message and P2P applications. To report on the above, Webwasher Content Reporter provides you with unprecedented visibility into your gateway traffic for Web, FTP, etc., to protect against spam, viruses, policy violations, and the like.

Specifications at a glance

Appliance and software deployments: Webwasher is available as high-performance turnkey appliances for every budget and performance demand as well as software for RedHat Enterprise and Suse Enterprise, Linux, Solaris, and Windows.

Supported WEB protocols: HTTP, HTTPS, FTP, and SMTP.

Supported IM & P2P protocols: Please see product information at *www.securecomputing.com/goto/webwasher.com*.

Bundled anti-malware engines: Sophos, McAfee, CA eTrust, Secure Anti-Malware.

OEM solutions: URL Filter list available for Network Appliance Netcache and Blue Coat ProxySG caching devices. An "in the cloud" filtering client is available for SnapGear™ SMB UTM devices.

Interfaces: Webwasher is fully ICAP compliant and can be deployed with any ICAP compliant gateway device.

* Source: IDC: Worldwide Secure Content Management 2006-2010 Forecast, March 2006, IDC# 200969

Plaintiff's Trial Exhibit
PTX-116
Case No. 06-369 GMS

Protections	Features	Customer benefit
Web misuse (Webwasher URL Filter on box a.k.a. "DynaBlocator")	On-box capabilities available for: • MS Internet Security & Acceleration server • SQUID caching server • Blue Coat ProxySG • Secure Computing® TSP and SnapGear™ firewalls	• Better productivity • HR/legal requirements • Additional line of defense against spyware and other malware entering through the corporate gateway • Blocks access to inappropriate Web sites
Web misuse (Webwasher [illegible])	All of the on-box capabilities above plus the following: • [illegible] • [illegible] • [illegible] • [illegible] Additional media type filtering capabilities • [illegible] • [illegible] Highly scalable	• Better productivity • HR/legal requirements • Additional line of defense against spyware and other malware entering through the corporate gateway • [illegible] available
Gateway anti-malware control/Policy enforcement (Webwasher)	• Includes full media type filtering capabilities as above • Secure Anti-Malware engine • Scans all Mail, Web, and FTP traffic Proactive security filters on active code • Digital signature check • Heuristics rule checker for malicious behavior • Heuristics rule checker for exploit methods and spyware • Prevents loss of confidential data • Text categorization (language) • Filters inbound and outbound	• Complements existing gateway AV scanner and firewall • Protects against spyware • Protects against day-zero and blended threats • Prevents loss of confidential data through the gateway for Web, FTP and Mail traffic • Allows acceptable language policy enforcement • One product for Web and Mail • Highly scalable, low TCO
Gateway anti-virus Inbound content control Policy enforcement (Webwasher)	• [illegible] • [illegible] • Highly scalable	• [illegible] • [illegible] • [illegible] • One product for Web and Mail
Spam, Phishing (Webwasher)	• Spam filter with all bells and whistles • Highly scalable • Superior detection rate, negligible false positive rate • 7 detection categories and millions of rules to detect spam • Near real-time updates of the spam filter • Tightly integrated to the other products of the suite • Added protection with integration of TrustedSource connection control technology	Any low-cost spam filter with excellent detection rates and dedicated phishing filtering
Instant Message and peer-to-peer file sharing abuse (Webwasher)	• [illegible] • [illegible] • [illegible]	[illegible]
Control over encrypted traffic (Webwasher SSL Scanner)	• Unlocks HTTPS traffic for scanning and reassembles afterwards for secure end-to-end communication • Enables enterprises to apply their existing security and Internet usage policies to all key Web protocols • Easily deployed on top of third-party gateway anti-virus or content protection solutions • Combination of filtering and certificate management policies for SSL (includes certificate checker) • Safely deployed [illegible] decrypted content on the wire • Highly scalable and easily available • Complies with strict European Union and international privacy regulations	Enables companies to close the HTTPS loophole at the gateway
Usage monitoring (Webwasher [illegible])	• [illegible] • [illegible]	• [illegible] • [illegible] • [illegible]

EXHIBIT 26
PART 1

10-K 1 d10k.htm FORM 10-K

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGEACT OF 1934**

FOR THE FISCAL YEAR ENDED DECEMBER 31, 2006

or

□ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SECURITIES EXCHANGEACT OF 1934**

For The Transition Period From To .

Commission file number 0-27074

SECURE COMPUTING CORPORATION
(Exact name of registrant as specified in its charter)

Delaware **(State or other jurisdiction of incorporation or organization)**	**52-1637226** **(I.R.S. Employer Identification No.)**
4810 Harwood Road, San Jose, California **(Address of principal executive offices)**	**95124** **(Zip code)**

Registrant's telephone number, including area code: (408) 979-6100

Joint Trial Exhibit
JTX-11
Case No. 06-369 GMS

Securities registered pursuant to Section 12(b) of the Act: None
Securities registered pursuant to Section 12(g) of the Act:
Common Stock, par value $.01 per share

Indicate by check mark if the Registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes □ No ☒

Indicate by check mark if the Registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes □ No ☒

Indicate by check mark whether the Registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the Registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No □

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of Registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☒

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definition of "accelerated filer and large accelerated filer" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerate filer □ Accelerated filer ☒ Non-accelerated filer □

Indicate by check mark whether the Registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes □ No ☒

The aggregate market value of the Common Stock held by non-affiliates of the Registrant as of June 30, 2006 was $426,485,662 based on the closing sale price for the Company's Common Stock on that date. For purposes of determining this number, all officers and directors of the Registrant are considered to be affiliates of the Registrant, as well as individual stockholders holding more than 10% of the Registrant's outstanding Common Stock. This number is provided only for the purpose of this report on Form 10-K and does not represent an admission by either the Registrant or any such person as to the status of such person.

As of March 12, 2007, the Registrant had 65,466,498 shares of Common Stock issued and outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the Registrant's Proxy Statement for its Annual Meeting of Stockholders to be held May 10, 2007 for the year ended December 31, 2006 are incorporated by reference in Part III hereof.

Table of Contents

TABLE OF CONTENTS

PART I

PART II

PART III

PART IV

Table of Contents

PART I

Forward-looking statements made in this Annual Report on Form 10-K or in the documents incorporated by reference herein that are not statements of historical fact are forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. The words "expect," "plan," "anticipate," "believe," "predict," and other similar expressions identify forward-looking statements. In addition, statements which refer to projections of our future financial performance, anticipated growth and trends in our business and other discussions of future events or circumstances are forward-looking statements. A number of risks and uncertainties, including those discussed in Item 1A under the caption "Risk Factors" in this Form 10-K and the documents incorporated by reference herein, could affect such forward-looking statements and could cause actual results to differ materially from the statements made. We do not undertake any obligation to update or correct any forward-looking statements.

In this Annual Report on Form 10-K, "Secure Computing," "we," "us," "our," and "Registrant" refer to Secure Computing Corporation.

ITEM 1. BUSINESS

We are a leading provider of enterprise gateway security solutions. Our best-of-breed portfolio of solutions provide Web Gateway, Messaging Gateway, and Network Gateway Security, as well as Identity and Access Management that are further differentiated by the proactive protection provided by TrustedSource™ (global intelligence). We are proud to be the security solutions provider to many of the most mission-critical and sensitive environments in the world. Our customers operate some of the world's largest and most sophisticated electronic business operations, and include prominent organizations in banking, financial services, telecommunications, healthcare, manufacturing, public utilities, and federal, state and local governments.

Across virtually all industries, organizations are using both the Internet and corporate private intranets and extranets to expand their business. This includes inbound access for remote employees, partners, and customers, as well as employees reaching beyond the edge of the internal network to communicate and gather information across the Internet. Our commitment is to support this method for exchanging information by mitigating risks and protecting information assets from the multitude of threats present on the Internet.

The bi-directional aspect of internet protocol (IP) based information exchange and application use creates a significant challenge for enterprises in terms of protection from malware, compliance with regulatory requirements, preventing data leakage, lost productivity, and the like. Given the sophistication of network and application-layer attacks, intelligence must be shared and leveraged across security applications. This intelligence must reflect, in *real time,* the changing security profile of the Internet, and flexible mechanisms to ensure regulatory compliance and reporting need to be hard-wired into the security infrastructure. We believe layered security or "defense-in-depth" needs to be viewed not only as a best practice for perimeter defense but also as something to be extended to mission-critical applications within the network. We define and implement a comprehensive set of gateway functions required to provide this necessary defense-in-depth for the primary mission-critical applications in the enterprise. This ongoing objective is at the heart of our mission.

We have formed partnerships with a number of companies in several different capacities. We make these solutions available to customers through the best and most advantageous channels possible, including solution providers, systems integrators, distributors, and companies who include our solutions in their product offerings. These companies include, for example: Alternative Technologies, AT&T, Blue Coat Systems, Cisco, Computer Associates, Comstor, Crossbeam, Dell, EDS, F5, Hewlett-Packard, McAfee, Microsoft, Network Appliance, NetOne Systems, Novell, PGP Corporation, SafeNet, Sun PS, SAIC, Tech Data, Voltage Security, Westcon, and Workshare.

Table of Contents

We operate our business within one operating segment called enterprise gateway security. For information regarding our revenue by geographical area, see Note 15 of the Notes to Consolidated Financial Statements. For information regarding the percentage of our revenue contributed by each of our product lines, see Item 7, *Management's Discussion and Analysis of Financial Condition and Results of Operations.*

Founded in 1989, we are incorporated in Delaware. Our principal executive offices are located at 4810 Harwood Road, San Jose, California 95124. Our telephone number at that location is (408) 979-6100. Our home page on the Internet is www.securecomputing.com. Other than the information expressly set forth in this annual report, the information contained, or referred to, on our website is not part of this annual report.

Acquisitions

On January 11, 2006, we completed our acquisition of CyberGuard Corporation, a leading provider of network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication, in a stock and cash transaction valued at $310.7 million. This acquisition strengthens our position as one of the market leaders in Network Gateway Security appliances, and strengthens our position in the Web Gateway Security space. CyberGuard was a logical fit for us, enhancing our strategic vision and better positioning us in two rapidly growing segments of the security industry. Along with an expanded customer and partner base, this merger provided us with important competitive advantages in the Network and Web Gateway Security markets.

On August 31, 2006, we completed our acquisition of CipherTrust, Inc., the global leader in the messaging security market, in a stock and cash transaction valued at $270.1 million. CipherTrust's products provide innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. CipherTrust's products include IronMail®, powered by TrustedSource™, IronIM™, Secure Computing Edge™, IronNet™, and RADAR™. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and messaging gateway security needs.

Industry Background

The rapid adoption of the Internet as a worldwide networking standard has accelerated the distribution and sharing of data and applications, enabling enterprises to adopt new electronic ways of doing business. The developing reliance on worldwide connectivity has allowed companies to greatly expand their business opportunities. Activities such as electronic trading of goods and services, online delivery of digital content, electronic funds transfers and share trading are now achieved in unprecedented ways. But with this growing opportunity comes new challenges for securing IT systems. The very features that give electronic business its power have elevated information security to a critical business issue.

Today's enterprise is no longer confined to a set of physical buildings; rather, the enterprise has become virtual. The Internet's power of connectivity has erased physical barriers, allowing an organization to establish ties around the globe. A business is no longer a single, isolated entity; it is part of a greater whole of interdependent entities whose lifeblood depends on the secure, electronic sharing of information. Organizations must now transcend the physical barriers of yesterday and expand their security measures *outward* to protect their digital resources beyond their physical buildings. They must also migrate their security measures *inward* to each individual's computer or laptop.

Table of Contents

Conducting Business Over Public Networks

As Internet-based infrastructure broadens, so do the risks associated with this exposure. These risks increase daily and threaten confidentiality, integrity, and secure availability of intellectual property, proprietary data, and computing resources. Such threats present themselves in many forms, including the following:

- Malicious attacks are becoming more sophisticated and continuing to increase in volume. According to International Data Corporation (IDC), a global provider of market research, malicious code, spyware and spam continue to be the most serious threats facing corporations today, but protecting sensitive data from leaving the organization is rapidly climbing the priority list of enterprise security threats.
- Hackers and attackers are no longer focused on hobby, but rather strict and prosperous financial gain, fraud and identity theft, which continue to be the leading drivers behind the increasing sophistication and volume of attacks.
- Web-based malware programs sent on infected pages or through email downloaded from Web-based mailbox or via embedded images can attack automatically and in real time, making Web security concerns a top priority for organizations seeking protection from the jump in spyware, Trojans, worms, and other Web-traffic attacks.
- Risks from exposure to malicious software, worms, and viruses that can enter networks from many sources and cause damage, install spyware, or open secret backdoors into private computing resources.
- Theft by both infiltrators and employees of private citizen records and other proprietary information in violation of numerous federal regulations and statutes and state and local statutes, such as Sarbanes-Oxley, the Gramm-Leach Bliley Act, and the Health Insurance Portability and Accountability Act.
- Intruders gaining unauthorized access to private computing resources and software applications.
- Legal liability exposure resulting from employee Internet access, or from hijacked use of desktop personal computers and servers for unauthorized file storage and file-sharing schemes.
- Identity theft and spoofing.
- Network and application server downtime due to denial of service (DoS) and distributed denial of service attacks (DDoS).
- Confidentiality leaks via email, instant messaging chat sessions, person to person file sharing, and unauthorized attachments that leave private networks unfiltered.
- Productivity losses from spam clogged email inboxes.

Application-Level Vulnerabilities

In today's highly complex Internet environment, network attacks have evolved into application-level attacks, and recently, an entirely new class of application-specific threats have arisen that require far more stringent protection. Protecting the network is highly important, but by itself, is not sufficient. The network is the foundation for communication, and the conduit over which people connect to the application resources they need and it is precisely these applications that can expose an organization's information resources to extreme vulnerability. Our products are designed to proactively address most, if not all, network security issues, whether its employees utilizing the Internet, or remote partners and customers accessing the intranet, Web services, and applications from outside the internal network. Our security measures extend beyond the network level, protecting applications and their resources so organizations can conduct their business, expand their reach, and drive success with confidence.

From email applications to Web services, File Transfer Protocol (FTP), customer relationship management (CRM) and sales force automation systems, people connect across networks to applications in order to conduct business every day. Misuse of applications and Web portals can result in the loss of valuable resources and

Table of Contents

millions of dollars. As the applications we use have become more sophisticated, so have the attack capabilities that threaten them. Applications contain inherent vulnerabilities, and sophisticated attackers can exploit these vulnerabilities and undermine an organizations' ability to conduct its business. Defensive measures must be even *more* sophisticated in their ability to protect against application-level threats—and our technology is designed with this in mind.

Along with protecting against known threats, today's security solutions must be able to anticipate unknown threats before they enter the network. A central part of an organization's business model must include provisions for safeguarding their business connections from being compromised to the highest degree possible.

Market Need and Strategy

More than ever before, organizations realize that they must take responsibility to protect their own confidential information and that of their customers and partners. Government regulations in recent years, such as the Federal Information Security Management Act, the Health Insurance Portability and Accountability Act, the Gramm-Leach Bliley Act, and the Children's Internet Protection Act, have heightened awareness and mandated that organizations secure their information across multiple segments—financial, medical, educational, and more. Enterprises must know that the data residing on a given network is secure and that parameters are in place for managing access to their proprietary information. Even as deadlines are met on these laws, enterprises must continue to refine their compliance solutions and move towards focusing on ongoing compliance. In the coming years, larger enterprises which had to put in a "quick fix" to meet deadlines will be looking to implement longer-term and more efficient solutions. Smaller businesses, which enjoyed some extended deadlines from Congress, are still implementing their first-time compliance solutions, representing a significant opportunity for security companies with a broad range of solutions.

Our strategy is to provide organizations, both at the enterprise level as well as the Small and Medium Business (SMB) level, with a broad set of solutions when it comes to implementing their security objectives, beginning with knowledge about security risks and regulations, accompanied by industry-leading security products to assist with mitigating these risks, and lastly, providing comprehensive security management capabilities. Our goal is to help organizations build confidence in the overall functionality and security of their network and application operations. We accomplish this by providing scalable, manageable, highly available solutions that meet their needs today and in the future. This objective includes meeting our customers' requirements for security products that provide broad solutions by integrating with each other and interoperate within current infrastructures. All of our products are designed to provide the strongest network protection available, along with central manageability, scalability, and interoperability.

Providing solutions that are manageable, easy to use and that lead the industry in total cost of ownership for the customer are our top objectives for organizations of all sizes. Our solutions enable best business practices that keep the workplace secure, productive, and easily manageable.

Our strategy also encompasses our award-winning service and support organization. We are able to provide our customers with unwavering service and support due, in part, to the knowledge base and technological expertise of our service and support staff.

Table of Contents

Secure Computing Solutions

Our specialized solutions are designed to meet customers' needs to balance security and accessibility, and to help them create trusted environments both inside and outside their organizations. Each of our products provide a complete solution in and of itself, and they also integrate with each other for a more comprehensive, unified, and centrally managed solution. We have developed a vision for comprehensive security on the enterprise gateway that embodies the following core design principles:

- **Appliance-based delivery.** All security functionality related to application intelligence and awareness needs to reside on a contained appliance. These appliances must be built on a secure operating system platform, have a regulated set of interfaces to external systems, and be encased in strong, tamper-proof hardware. Essentially, the appliance must mitigate the many security management problems of deploying software on a standard operating system-server configuration.
- **Application and content awareness.** Today's security attacks have progressed far beyond the network and protocol level to that of the application and content. The gateway needs a deep knowledge of the underlying communication, an understanding of the context of the communication, and the ability to inspect and interpret the content.
- **Centralized policy, management and reporting.** The security gateway must have the ability to be centrally configured, provisioned and managed. This, along with consolidated reporting, should provide immediate feedback on the effectiveness of the security appliance while helping reduce the cost of ownership.
- **Bi-directional protection.** The security gateway needs to effectively scrutinize inbound traffic in order to block bad traffic from entering the network, while simultaneously performing deep inspection of outbound content to protect against leaks of confidential information or intellectual property.
- **Proactive protection.** With the rapid increase in polymorphic threats, the ability to know immediately what could be dangerous is imperative. A gateway security system should be able to effectively thwart these attacks in real time.
- **User management and education.** The security gateway needs to protect all types of sensitive data automatically, with easy-to-manage policies, comprehensive audit trails, and employee feedback loops.
- **Performance.** As traffic volumes increase exponentially, the gateways must be able to keep up and scale for performance without having to replace them, or take them off-line for major upgrades.
- **Resiliency.** Security gateways should not introduce points of failure to the mission at hand.

Our solutions for securing critical connections fall into four categories: TrustedSource Global Intelligence, enterprise gateway security appliances (Network, Web, and Messaging Gateways), Identity and Access Management, and Security and Support services.

TrustedSource Global Intelligence

We believe TrustedSource technology is the most precise and comprehensive Internet host reputation system in the world, which we are rolling into many of our product lines as a key cornerstone of Global Intelligence security. TrustedSource characterizes Internet traffic and makes it understandable and actionable, and also creates a profile of all "sender" behavior on the Internet and then utilizes this profile to watch for deviations from expected behavior for any given sender. TrustedSource then calculates a "reputation score" based on the behavior of the sending host. We have an extensive network of thousands of sensors and other collection vehicles throughout the Internet which tracks and reports back to TrustedSource, data on all observed email traffic, giving TrustedSource a real-time view of Internet communication worldwide.

Originally developed to identify spammers, TrustedSource is able to recognize any "host" profile anomalies and immediately calculate new reputation scores for senders and propagate this information to all TrustedSource

Table of Contents

clients. Analyzing not only email senders but Internet domains as well, this Global Intelligence technology is able to profile literally millions of entities connected to the Internet worldwide in real-time, and provide up-to-the minute host behavior analysis. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists and network characteristics with the unparalleled strength of our global network. We believe the result is the most complete reputation system in the industry with the ability to score every IP address across the Internet.

Enterprise Gateway Security Appliances

Network Gateway Security

Our enterprise gateway security platforms are the aggregation points not only for application-specific defense-in-depth technologies based on deep knowledge of the underlying protocols and application environment, but also a mechanism for introducing real-time intelligence to security-relevant decisions about the disposition of application-specific traffic. This incorporates host and domain intelligence as well as bi-directional security services in the areas of compliance, policy, encryption, email, Web, and anti-malware protection. These services leverage centralized policy and management and are fully integrated with TrustedSource and SafeWord® Identity and Access Management technology.

The idea of the network perimeter has evolved significantly since the advent of the Web. A mobile workforce, extranets, distributed applications and an environment of highly sophisticated, blended threats has forced enterprises to deploy an array of separate security applications to provide services such as firewall, Virtual Private Network (VPN), Intrusion-Detection System (IDS)/Intrusion-Prevention System (IPS), anti-virus, anti-spam, and more. The recent movement toward all-in-one appliances has helped mitigate the problem to an extent, especially for small and mid-size companies, but three major issues still remain: 1) many solutions rely on known malware signatures and fail to offer protection against previously unknown attacks 2) the Internet is a dynamic environment, with a security profile that changes in real time, and 3) enterprise security applications often fail to adequately share policy and application intelligence between one another. Our Network Gateway Security products address each of these areas of concern, providing the industry's strongest application firewall protections.

Sidewinder G2 Security Appliance—Our security appliances consolidate all major Internet security functions into a single system. Sidewinder G2® defends the network against all types of threats, both known and unknown. Through its unified threat management (UTM) approach, Sidewinder delivers best-of-breed anti-spyware, anti-virus, anti-spam and anti-fraud engines, Web content filtering, TrustedSource IP reputation services, secure Domain Name System (DNS), VPN, and Secure Sockets Layer (SSL) gateways, and more.

In 2006, we continued to differentiate our UTM appliance from the competition with demonstrable zero-hour attack protections on high profile Internet attacks (such as the Sendmail vulnerability in March and Microsoft Windows MetaFile "WMF" attack in January). We also announced plans to merge our newly-acquired CyberGuard® Firewall/VPN technologies (TSP and Classic) with our Sidewinder G2 Security Appliance in our next generation UTM appliance that has come to market in the first quarter of 2007. The CyberGuard acquisition also brought to us a new paradigm in enterprise central management with the Command Center which we will continue to leverage going forward. We believe Command Center's ability to do administration, configuration, monitoring, and management of software updates for a global appliance deployment coupled with our Security Reporter product's central reporting, and full out-of-the box compliance reports, continue to ensure that both medium and large customers see our network gateway appliances as the product of choice.

Sidewinder G2 continues its proven security track record, in great part due to our SecureOS® operating system with our patented Type Enforcement® technology and flexible application level protection mechanisms. In 2006, our accomplishments of FIPS 140-2 validation and continued leadership with Common Criteria (CC) EAL4+ certification for application level firewalls puts us in an unparalleled class of product when competing in the U.S. and other government opportunities all around the world.

Table of Contents

CyberGuard Total Stream Protection (TSP)—Like Sidewinder G2, CyberGuard Total Stream Protection (TSP) line of UTM appliances is designed to protect mid-size to large enterprises against both known and zero-hour attacks, using a hybrid architecture that combines stateful packet filtering, seven layer inspection, and secure content policy enforcement. The devices include a fully integrated IPSec VPN, flexible authentication and advanced filtering strategies. Sidewinder G2 and TSP share common hardware.

SnapGear—SnapGear™ security appliances integrate networking, firewall, intrusion prevention security, and remote access requirements into one small form-factor appliance, fulfilling the lower end of the pricing scale of our network gateway security line of products. Designed to provide a complete office-in-a-box networking device for small and mid-sized organizations, SnapGear is the only networking device needed for office PCs to be networked with one another, connect securely to the Internet, connect to the corporate WAN, and service all remote access VPN needs, thereby providing small and midsize businesses with enterprise-level networking capabilities.

Web Gateway Security

Web Gateway Security appliances protect enterprises from malware, data leakage, and Internet misuse, while helping to ensure policy enforcement, regulatory compliance, and a productive application environment. These platforms analyze traffic bi-directionally. Inbound, they isolate and eliminate threats from all types of malware, including zero-day threats, viruses, Trojans, spam, phishing, and the like. They use a deep knowledge of the underlying protocols and application behavior combined with global intelligence to make security decisions. On the outbound side, in addition to preventing virus propagation and unwanted Web site access, our enterprise Web Gateway Security helps customers achieve regulatory compliance and prevent data leakage across both Web and messaging applications.

Webwasher—Webwasher® Web Gateway Security appliances provide best-of-breed content security to secure Web-based enterprise traffic. Webwasher provides URL filtering to block access to inappropriate Web content and help prevent phishing attacks, and provide malware protection with Proactive Security technology to guard against zero-day attacks and blended threats. Webwasher also features SSL Scanning which identifies and blocks malicious content hidden in SSL-encrypted traffic from accessing the network and confidential information from leaving the network. All products can be managed from a single Web Graphical User Interface (GUI) and Content Reporter offers enterprise-class reporting on all Webwasher products and most gateway cache appliances and firewalls. In 2006, and continuing into 2007, WebWasher has begun integration, and will continue, to integrate SmartFilter for its current and future URL filtering capabilities.

SmartFilter—Our flagship URL filtering application, SmartFilter®, is an enterprise solution currently shielding thousands of organizations from inappropriate use of the Web and the security threats often associated with viewing inappropriate, malicious or infected Web sites. SmartFilter provides deployment and platform flexibility with over 30 different options including leading firewalls, security appliances, proxy servers or caching systems. SmartFilter continues to be the de facto filtering standard for original equipment manufacturers (OEM). SmartFilter is integrated on market-leading solutions from vendors such as McAfee and Computer Associates.

Messaging Gateway Security

Messaging has undergone a fundamental change in enterprise environments. Not too long ago, most electronic messaging was confined to applications like Microsoft Outlook and Lotus Notes. Now with the advent of Web-based mail applications like hotmail and gmail, as well as instant messaging, there are many more channels both into and out of the enterprise network. In fact, messaging is now the preferred attack vector for hackers, and spam is their weapon of choice. Hackers now employ sophisticated networks of thousands of "zombie" computers or "botnets" to send messages infected with malware, putting the enterprise at a significant disadvantage. Even more discouraging is the sharp rise in zero-day attacks, where there is no known signature that can be used to block the attack.

Table of Contents

Furthermore, messaging now represents a bi-directional challenge. Not only are inbound threats becoming much more sophisticated and targeted, but outbound data leakage and regulatory compliance have become huge and well-publicized liabilities for enterprises. Users can easily attach confidential documents to emails and Instant Message (IM) conversations, making it trivial for sensitive information to find its way outside the network. Outbound content checking is not common practice. And even in instances where such controls are in place, where the enterprise user is communicating over an SSL-encrypted link (i.e., HTTPS), there is typically no mechanism in place to decrypt and inspect the traffic to ensure that policies are being enforced.

Recognizing that messaging is now a primary business application in most enterprises, we have implemented a strategy to comprehensively address both inbound and outbound threats and to help our customers insure compliance with federally mandated requirements for the protection of sensitive data. Our Messaging Gateway Security platforms look at traffic bi-directionally. Inbound, they proactively isolate and eliminate threats from all types of malware—zero-day threats, viruses, Trojans, spam, phishing, and the like. We use a deep knowledge of the underlying protocols and application behavior combined with real-time global intelligence to add a new dimension to security-related processing.

On the outbound side, through sophisticated fingerprinting and data profiling techniques, our Messaging Gateways are able to determine which data (either in the form of text in a message or text within an attachment) need to be blocked or flagged due to security or compliance concerns. Our Messaging Gateways can also enforce mandatory outbound encryption for certain traffic types without requiring the installation of client software on the recipient's system. We also prevent virus propagation throughout the messaging infrastructure, delivering maximum availability and security, effectiveness and global enterprise manageability across multiple messaging protocols including email, instant messaging and Webmail. This combination of easy-to-manage gateway appliances and sophisticated, centralized real-time network intelligence provides clean, efficient communications, eliminating both inbound and outbound risks.

IronMail—IronMail® provides a centrally managed, integrated, best-of-breed messaging gateway security appliance for enterprises of all types and sizes. In one integrated appliance, IronMail protects enterprise email systems from inbound (spam, viruses, phishing, and hackers) as well as from outbound threats (regulatory or corporate policy compliance violations or theft/leakage of confidential information or intellectual property). We have integrated TrustedSource IP reputation identities into our IronMail Messaging Gateway Security appliances to provide real-time behavior analysis on more than one-third of the world's enterprise messaging traffic with over 7,000 sensors located in 48 countries.

IronIM—The IronIM™ instant messaging security appliance is the first and only solution that integrates policy to secure, log, monitor, and encrypt enterprise IM communications. IronIM allows administrators to control and manage the use of public and enterprise IM from a single management platform to eliminate risks from IM-borne threats, ensure compliance with various industry and government regulations, and monitor for information leakage or other policy violations. IronIM supports multiple instant messaging networks (including AOL Instant Messenger, MSN Messenger, Yahoo! Messenger, and corporate IM solutions including Microsoft LCS and IBM SameTime) and does not require deployment of a new IM client.

RADAR—RADAR™ protects an organization's online reputation, whether by detecting and stopping phishing scams or identifying and fixing PCs. RADAR receives a real-time stream of behavior-based intelligence from our TrustedSource global threat correlation engine to detect deviations from expected behavior for all senders and provides real-time alerting to customers.

Secure Computing Edge—Secure Computing Edge™ is a hardened appliance positioned at the perimeter of the mail system, applying TrustedSource technology to control email traffic at the network border rather than at the mail server or desktop. Edge relies on TrustedSource for information about every sender, to allow or reject email before it even reaches critical mail servers.

Table of Contents

Identity and Access Management

One important development in enterprise security has been recognition of the need for strong authentication as a prerequisite for access to corporate network resources (either remotely or from inside the network). Strong authentication has now been coupled with a fully-functional access gateway and the ability to coordinate policies governing the extent and scope of corporate resource access by individuals. This combination of strong authentication, centralized policy management and the ability to report at a very granular level on security-relevant activity is commonly referred to as Identity and Access Management (IAM), and is fundamental to any corporate security strategy.

We expanded our SafeWord® product line in 2006, thereby providing a comprehensive Identity and Access Management portfolio that is fully integrated into our enterprise gateway security strategy and provides strong authentication and centralized policy and reporting across the entire enterprise gateway security portfolio.

Remote access to network resources is a requirement for many businesses, but verifying the identity of your remote users with strong authentication and a reliable identity management system is vital for security. Additionally, organizations are increasingly realizing the many vulnerabilities of passwords, and they require strong authentication systems that are easy to install and deploy, simple to manage, and able to grow with their needs.

Our SafeWord products meet these needs. By providing safe access to applications, data, and resources through policy-driven security initiatives, as well as positively identifying users through strong authentication, SafeWord products assure that only the right people can make connections to an organization's applications and resources. SafeWord software and SafeWord tokens offer flexibility, scalability, and ease of use, and are used by thousands of organizations and millions of end users worldwide every day.

SafeWord SecureWire—In April 2006, we broadened our presence in the authentication market into the IAM space by introducing our SafeWord SecureWire™ appliance. IDC defines the IAM market as a comprehensive set of solutions used to identify users in a system and control their access to resources within that system by associating user rights and restrictions with the established identity. SafeWord SecureWire is a new, robust technology that functions as the access, authentication, and compliance hub for the entire network. SecureWire is designed to simplify access to applications, data, and network resources by hosting and managing all external access methods on a single appliance, such as, VPNs, Citrix applications, extranets, and Webmail. SecureWire can also host and manage all internal access methods: LAN connections, wireless LANs, and even mainframes. By providing secure access management inside and outside the virtual perimeter, and by consolidating all policies on a single device, SecureWire helps enable our customers to achieve configuration compliance because only properly configured devices are allowed to access their networks.

We include SafeWord strong authentication tokens with every SecureWire shipment to allow customers to provide proof-positive identity of all users entering their network. SecureWire is also available in a wireless package, now bundled with our SnapGear wireless appliance to provide a complete wireless access management system. The access appliance also delivers a reliable mechanism to enable configuration compliance, enforcing every end-point device to adhere to corporate IT policy, including work PCs, laptops, home PCs, and workstations. SecureWire allows our customers to mandate that only properly configured, properly secured devices are granted access according to their security policy, and to ensure that system patches, anti-virus software, and firewall protection are all in place.

SafeWord PremierAccess is our leading strong authentication solution for Microsoft environments using Active Directory, providing proof-positive user identities via VPNs, Citrix applications, Outlook Web Access, Windows Domain and Terminal Services logins. SafeWord PremierAccess® offers powerful management tools with the Enterprise Solution Pack (ESP), an optional add-on package that provides advanced user management, support for a wide range of authentication form factors, advanced reporting capabilities, and rich access control functionality.

SafeWord RemoteAccess is a simple, easy-to-use strong authentication solution designed to protect VPN, RADIUS, Citrix, and Outlook Web Access connections. With tight integration and simplified management through Active Directory, and with tokens that generate new passcodes with every user login, SafeWord RemoteAccess™ lets you easily and cost-effectively eliminate the password risk. RemoteAccess is available in the following branded versions: SafeWord RemoteAccess, SafeWord RemoteAccess-Cisco compatible, SafeWord for Citrix, SafeWord for Check Point, and SafeWord for Nortel Networks.

Security and Support Services

Our services are designed to ensure that our customers make optimal use of our products when controlling access to their networks and applications. We provide a life cycle of support and services, including: Solution Planning, Solution Implementation, and Solution Support. These services are described below.

Solution Planning—Our Security Services offerings include a variety of options for rapid assessment of a company's current network architecture and evaluation of the current status of network security. We then compare this information to the company's business needs, both current and future, to help them plan a scalable and secure e-commerce solution. In addition, we offer security policy services that help customers prepare a policy and plan that transfers their security policy from paper to practice. We provide the following services: network architecture security assessment; security policy assessment and development; and product and audit configuration assessment.

Solution Implementation—Our Network Services team offers a full range of rapid-deployment integration services and training to assist our customers through implementation and integration of our products. Both the configuration process of a security system and the security products themselves, by their nature, may have an impact on several areas within a customer's network. Accordingly, we offer a complete package of product integration assistance to ensure our customers maximize network uptime and maintain productivity during the process. We provide the following services: product implementation; product audit and configuration; and product training.

As part of our Network Services training program, we provide extensive product and network training online through our Web-based classes. In addition, we offer hands-on training at our training facilities, and these classes are also available worldwide onsite for our customers and partners. These services help our customers understand basic and advanced administration rules and tools that enable partners to configure, integrate, and maintain our products as part of a comprehensive e-business solution.

Solution Support – SecureSupport®—We offer industry leading live answer support services. SecureSupport has a team of technical support engineers that provide customer support around the clock via email, the Web, or telephone. Service options are tailored for each of our enterprise gateway security products and customer requirements. Customers can select the SecureSupport option that best meets their needs. Our support center call statistics are published and posted to our corporate Web site at www.securecomputing.com.

We designed SecureSupport Online, a tool to assist our customers and channel partners with any problem they may experience with any of our products. Through this process, technical expertise is offered online through a searchable knowledge base, viewable support history, and email access. Product patches and release notes can also be downloaded.

We offer our customers the option to purchase software support and upgrade service for an annual fee. We provide software updates and technical support through this program.

Customers

Our expanded global footprint now encompasses more than 19,000 customers operating some of the largest and most sensitive networks and applications in the world. Our partners and customers include the majority of

Table of Contents

the Dow Jones Global 50 Titans and numerous organizations in the Fortune 1000, as well as banking, financial services, healthcare, real estate, telecommunications, manufacturing, public utilities, schools, and federal, state and local governments. We have relationships with the largest agencies of the U.S. government. Our customer list also includes numerous international organizations and foreign governments. Overseas, our customers are concentrated primarily in Europe, Japan, China, the Pacific Rim, and Latin America.

No customer accounted for more than 10% of our total revenue in 2006, 2005 or 2004.

Sales

We sell our products and services both directly and indirectly through domestic and international distributors, value-added resellers, major integrators, and OEMs. For 2006, sales to major end users comprised 19% of total sales, while indirect channel sales comprised 81%. Our sales organization is divided geographically into the following territories: North America; Federal; Europe, the Middle East and Africa; Asia Pacific; and Latin America.

Our market strategy promotes our PartnersFirst reseller program, a channel program through which nearly all of our global indirect business is conducted. The program reflects our commitment to a partner-focused sales model and enhances access to our products by making them available through over 2,000 resellers via leading distribution partners and streamlined processes. Our channel program makes the process of doing business with us simple, while giving partners enhanced abilities to increase revenue.

We have a U.S. federal government sales team and a General Services Administration (GSA) schedule for our products maintained by a third party, to facilitate government orders. The U.S. government is the world's largest buyer of security products and continues to be a strong market for us.

The following table summarizes our products and services revenues (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Revenues:			
Products	$115,628	$ 79,339	$67,625
Services	61,069	29,836	25,753
	$176,697	$109,175	$93,378

Marketing

We market our products to existing customers and prospects worldwide using a variety of integrated marketing programs. Our marketing team creates and implements marketing campaigns in each of our major functional market areas: corporate marketing for company and brand awareness, product marketing, and partner marketing.

By leveraging relationships with our channel partners, we generate sales leads and brand awareness through customer focused initiatives. Additionally, we work closely with industry analysts and current customers to understand the trends and needs associated with the enterprise gateway security marketplace. Our research and experience help drive key marketing initiatives including: direct marketing, Web marketing, print advertising, customer seminars, Web seminars, and trade shows. We also work closely with outside vendors to help us pre-qualify leads in order to provide our partners with well qualified prospects.

An active international public relations program ensures that we receive appropriate press coverage for our various programs and announcements as well as obtain product reviews and speaking engagements. In addition to our marketing programs, we stimulate interest and demand for our solutions through our corporate Web site,

Table of Contents

channel partner Web sites and other industry-specific Web sites, providing white papers, newsletters, and technical notes. Several of our senior technical staff contribute articles to industry periodicals as well as abstracts for presentations they provide to industry specific summits and events, further extending our ability to educate the industry about e-business security.

Competition

The market for enterprise gateway security is highly competitive and we expect competition to intensify in the future. Our products compete on the basis of quality of security, ease of installation and management, scalability, performance and flexibility. Each of our individual products competes with a different group of competitors and products. Current significant competitors for our existing products include: Check Point Software Technologies Ltd.; Cisco Systems, Inc.; Fortinet, Inc.; Juniper Networks; EMC Corporation (formerly RSA Security, Inc.); VASCO Data Security International, Inc.; SonicWall; SurfControl, plc; Blue Coat Systems, Inc.; Symantec Corporation; Postini, Inc.; Tumbleweed; IronPort Systems, Inc.; and Websense, Inc.

Seasonality

As is typical for many large software companies, a part of our business is seasonal. A slight decline in product orders is typical in the first quarter of our fiscal year when compared to product orders in the fourth quarter of the prior fiscal year. In addition, we generally receive a higher volume of orders in the last month of a quarter. We believe this seasonality primarily reflects customer spending patterns and budget cycles.

Backlog

Our backlog for products at any point in time is not significant since products are shipped upon receipt of order. We do not believe that our backlog at any particular point in time is indicative of future sales levels. The timing and volume of customer orders are difficult to forecast because our customers typically require prompt delivery of products and a majority of our sales are booked and shipped in the same quarter. In addition, sales are generally made pursuant to standard purchase orders that can be rescheduled, reduced, or canceled prior to shipment with little or no penalty.

Manufacturing

Our manufacturing operations consist primarily of light manufacturing of our software and appliance products. We use subcontractors to duplicate software media and print user documentation and product packaging for our software products. We have two different processes for manufacturing our appliances depending on the product line. We either procure computer servers from major computer manufacturers and then assemble the final software and hardware products at our facilities in St. Paul, Minnesota or we outsource all services to third party providers. The third party providers complete the hardware build per our configuration specifications, perform a final test, and then image and drop ship the product directly to our customers.

Our SafeWord product line includes a small token, available in various designs. We source these tokens through electronics assembly manufacturers located in China.

The majority of the materials used in our manufacturing operations are industry-standard parts. Typical materials required are media and media duplication services, user documentation and other printed materials, product packaging, and computer systems (computer servers, computer peripherals, memory disk drives, and storage devices).

Research and Development

Our internal engineering staff performs internal development of new products and features. For the years ended December 31, 2006, 2005, and 2004, our research and development expenses were $34.1 million, $16.8 million, and $16.1 million, respectively.

Table of Contents

We intend to keep our products broadly compatible with industry standards, other information security products and other applications. In addition, we will introduce new products as market demand develops for such products. We design our products so that they support emerging or evolving security and content standards, such as Hypertext Transfer Protocol (HTTP), Extensible Markup Language (XML), Simple Mail Transfer Protocol (SMTP), the Public Key Cryptography Standards (PKCS), IPSec, Lightweight Directory Access Protocol (LDAP), Internet Protocol Version 6 (IPv6), Secure Sockets Layer (SSL), and others.

Patents and Proprietary Technology

We rely on patent, trademark, copyright, and trade secret laws, employee and third party nondisclosure agreements, and other methods to protect our proprietary rights. We currently hold a number of U.S. and foreign patents relating to computer security software and hardware products. We believe that our patents are broad and fundamental to information security computer products.

Our success depends, in part, upon our proprietary software and security technology. We also rely on trade secrets and proprietary expertise that we seek to protect, in part, through confidentiality agreements with employees, consultants, and other parties.

We have used, registered, and/or applied to register certain trademarks and service marks to distinguish genuine Secure Computing products, technologies and services from those of our competitors in the U.S. and in foreign countries and jurisdictions. We enforce our trademark, service mark and trade name rights in the U.S. and abroad.

Employees

As of December 31, 2006, we had 885 employees. Of these employees, 341 were involved in sales and marketing, 123 in customer support and services, 269 in research and development, 58 in production, 39 in information technology and 55 in administrative, human resources and finance. None of our employees are represented by a labor union or is subject to a collective bargaining agreement. We believe that we maintain good relations with our employees.

Executive Officers

Our executive officers and their ages as of March 12, 2007 are as follows:

EXECUTIVE OFFICERS	AGE	POSITION WITH SECURE COMPUTING CORPORATION
John E. McNulty	60	Chief Executive Officer, President and Chairman of the Board
Jay S. Chaudhry	48	Vice Chairman and Chief Strategy Officer
Timothy J. Steinkopf	45	Senior Vice President of Operations and Chief Financial Officer
Vincent M. Schiavo	49	Senior Vice President of Worldwide Sales
Michael J. Gallagher	43	Senior Vice President of Product Development
Mary K. Budge	51	Senior Vice President, Secretary and General Counsel
Dr. Paul Q. Judge	30	Chief Technology Officer
Atri Chatterjee	44	Senior Vice President of Marketing

JOHN E. MCNULTY is our Chairman, President and Chief Executive Officer. Mr. McNulty first joined us as President and Chief Operating Officer in May 1999 and assumed the positions of Chairman of the Board and Chief Executive Officer in July 1999. From 1997 until joining us, he served as Senior Vice President of Sales, Services, and Business Development at Genesys Telecommunications Laboratories. Mr. McNulty was also previously with Intel Corporation, where he held a number of positions, including Director of Marketing and Business Development for the Enterprise Server Group, which he launched.

Table of Contents

JAY S. CHAUDHRY is our Vice Chairman and Chief Strategy Officer. Mr. Chaudhry joined us in August 2006 as a result of our acquisition of CipherTrust, Inc. which he founded in 2000 and where he served as Chief Executive Officer. Prior to that, his experience includes sales, marketing and engineering experience with IBM, NCR and Unisys Corporation, and the successful launch of several technology companies.

TIMOTHY J. STEINKOPF is our Senior Vice President of Operations and Chief Financial Officer. Mr. Steinkopf first joined us as Treasurer and Director of Investor Relations in September 2000 and assumed the positions of Vice President and Chief Financial Officer in March 2001. Mr. Steinkopf was appointed to Senior Vice President in January 2002. From 1999 until joining us, he was at Silicon Entertainment, Inc. where his last position was Chief Financial Officer and Vice President of Finance. He was the Vice President of Finance, Secretary and Treasurer at Watt/Peterson Inc. from 1991 to 1999. Prior to that, he was at Ernst & Young LLP.

VINCENT M. SCHIAVO is our Senior Vice President of Worldwide Sales. Mr. Schiavo joined us in April 2001. From 1998 until joining us, he served as President of PolyServe, Inc. Prior to that he served as Vice President of Worldwide Sales at Sonic Solutions and in various other sales management roles at Radius, Apple Computer and Data General Corporation.

MICHAEL J. GALLAGHER is our Senior Vice President of Product Development. Mr. Gallagher rejoined us as Vice President and General Manager of our Network Security Division in 1999 and assumed the position of Senior Vice President of Product Development in August 2003. From 1997 until rejoining us, he was the Vice President of Software and Systems Engineering at Datakey. In 1996 and into 1997, he was employed by us and was responsible for management of several firewall and security initiatives. Prior to that he held various software engineering and technical management positions with increasing responsibility at Unisys Corporation.

MARY K. BUDGE is our Senior Vice President, Secretary and General Counsel. Ms. Budge joined us in November 1996 as corporate counsel and was appointed Senior Vice President in February 2005. Prior to joining us, she was an attorney for Schwegman, Lundberg, Woessner & Kluth where she specialized in trademark and copyright law. Ms. Budge is a member of the Minnesota Bar Association and the American Corporate Counsel Association.

DR. PAUL Q. JUDGE is our Chief Technology Officer. Mr. Judge joined us in August 2006 as a result of our acquisition of CipherTrust, Inc., where he served as Chief Technology Officer since 2000. Prior to that, he worked with IBM and NASA.

ATRI CHATTERJEE is our Senior Vice President of Marketing. Mr. Chatterjee joined us in August 2006 as a result of our acquisition of CipherTrust, Inc., where he served as Senior Vice President of Marketing since April 2006. From September 2003 until joining CipherTrust, he co-founded Mercora and served as the Vice President of Marketing and Business Development. In 2001 and into 2003, he served as the Vice President of Marketing and Business Development for McAfee.

None of the executive officers are related to each other or to any other director of Secure Computing.

Other

Our Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to those reports are available, free of charge, on our website at www.securecomputing.com as soon as reasonably practicable after they are filed with the SEC.

The public may also read and copy any materials we file with the SEC at the SEC's Public Reference Room at 100 F Street, NE, Room 1580, Washington, DC 20549. The public may obtain information on the operation of the Public Reference Room by calling the SEC at 1-800-SEC-0330. The SEC also maintains a website at www.sec.gov that contains reports, proxy and information statements, and other information regarding issuers, such as us, that file electronically with the SEC.

Table of Contents

ITEM 1A. RISK FACTORS

The following important factors, among others, could cause actual results to differ materially from those indicated by forward-looking statements made in this Annual Report on Form 10-K and presented elsewhere by us from time to time.

We may be unable to integrate our operations successfully and realize all of the anticipated benefits of the mergers with CipherTrust and CyberGuard. Our mergers with CipherTrust and CyberGuard involve the integration of companies that previously have operated independently, which is a complex, costly and time-consuming process. The difficulties of combining the companies' operations include, among other things:

- Coordinating geographically disparate organizations, systems and facilities;
- Integrating personnel with diverse business backgrounds;
- Consolidating corporate and administrative functions;
- Consolidating research and development, and manufacturing operations;
- Coordinating sales and marketing functions;
- Retaining key employees; and
- Preserving the research and development, collaboration, distribution, marketing, promotion and other important relationships of the companies.

The process of integrating operations could cause an interruption of, or loss of momentum in, the activities of the combined company's business and the loss of key personnel. The diversion of management's attention and any delays or difficulties encountered in connection with the merger and the integration of the two companies' operations could harm the business, results of operations, financial condition or prospects of the combined company after the mergers. We believe that the operation integration of CyberGuard is essentially complete. However, as of December 31, 2006, we have only twelve months of combined operations, and we may, in the future, encounter again any or all of the difficulties in operation integration we have faced in the period since the merger with CyberGuard, particularly due to the ongoing integration of CipherTrust. We expect the integration of CipherTrust to be completed in 2007.

We have experienced operating losses in the past and may experience operating losses in the future. In 2006 we incurred operating profit of $769,000 in the quarter ended March 31, 2006 and operating losses of $2.7 million, $6.3 million, and $9.5 million in the quarters ended June 30, 2006, September 30, 2006, and December 31, 2006, respectively. In 2005 we had continuing operating profit, although we have incurred operating losses in the past. If we are unable to attain operating profits in the future, our stock price may decline, which could cause you to lose part or all of your investment.

In 2006 we were cash flow positive, however, we have experienced negative cash flow in the past and may experience negative cash flow in the future. If, at that time, sources of financing are not available, we may not have sufficient cash to satisfy working capital requirements. We believe that we have sufficient financial resources to satisfy our working capital requirements for at least the next twelve months. We may seek to sell additional equity or debt securities or obtain an additional credit facility at that time or sooner if our plans change or if we expend cash sooner than anticipated. Any additional financing may not be available in amounts or on terms acceptable to us, if at all. Our failure to obtain financing at that time could result in our insolvency and the loss to investors of their entire investment in our common stock.

If we fail to meet the borrowing requirements under our credit agreement, we may be unable to obtain necessary short-term financing and if we default on a secured loan, material assets of ours could be subject to forfeiture. We currently are party to a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank which provides us with a $90.0 million term loan facility, a $20.0 million revolving credit facility and a swingline loan sub-facility. As of December 31, 2006, we had $88.0 million of outstanding indebtedness. Of this indebtedness, approximately $28.0 million bears interest at rates that fluctuate with changes in certain prevailing interest rates. An increase in interest rates would have a negative impact on our earnings due to an increase in interest expense. As is typical for credit facilities of this sort, the credit agreement for such credit facility imposes certain restrictions on us, including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit agreement requires us to comply with certain financial covenants, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We can offer no assurances that we will be able to comply with such financial covenants when a loan is needed or continue to comply with such covenants when a loan is outstanding. If we fail to satisfy these covenants or if we are unable to meet the conditions for borrowing under our credit agreement when funds are required, we could be prevented from meeting our payment obligations, which could have a material adverse effect on our business, financial conditional and operating results.

Further, our obligations under the credit agreement are secured by substantially all of our material assets, including real and personal property, inventory, accounts, intellectual property and other intangibles. If we default under our credit agreement for any reason and are unable to cure the default pursuant to the terms of the credit agreement, our lenders could take possession of any and all of our assets in which they hold a security interest, including intellectual property, and dispose of those assets to the extent necessary to pay off our debts, which could materially harm our business.

Our significant stockholders could have significant influence over us. Warburg Pincus beneficially owns 100% of the outstanding shares of Secure Computing Series A Preferred Stock convertible into approximately 5.7 million shares or 7.0% of Secure Computing common stock on a fully diluted basis. The shares of Series A Preferred Stock are convertible into shares of our common stock at the holder's option, at a rate determined by dividing the aggregate liquidation preference of the shares of Series A Preferred Stock to be converted by $12.75. This liquidation preference, and the shares of common stock issuable upon conversion of the Series A Preferred Stock, accretes at the rate of 5% per year, compounded semi-annually over time. Subject to certain exceptions and limitations, the liquidation preference shall accrete for 54 months from the date of issuance, giving Warburg Pincus approximately 6.7 million shares, or 8.2% of our company on a fully accreted basis. Also, Warburg Pincus holds a warrant to purchase 1,000,000 shares of common stock at an initial per share exercise price of $13.85. Additionally, Warburg Pincus is entitled to nominate a member to our board of directors and the consent of the holders of the Series A Preferred Stock is required for certain corporate actions.

Jay Chaudhry, Vice Chairman of the Board and Chief Strategy Officer, beneficially owns 5,252,636 shares of Secure Computing common stock, or 6.4% of Secure Computing common stock on a fully diluted basis. Richard Scott, a member of our Board of Directors, beneficially owns 3,977,431 shares of Secure Computing common stock, or 4.9% of Secure Computing common stock on a fully diluted basis.

Accordingly, Warburg Pincus, Jay Chaudhry, and Richard Scott could significantly influence the outcome of any corporate transaction or other matter submitted to the stockholders for approval. The interests of Warburg Pincus, Jay Chaudhry, and Richard Scott may differ from the interests of other stockholders.

Holders of our Series A Preferred Stock have rights that are senior to those of our Common Stock. Holders of our Series A Preferred Stock are entitled to receive benefits not available to holders of our common stock. These benefits include, but are not limited to, the following:

- beginning July 2010, shares of Series A Preferred Stock will be entitled to receive semi-annual dividends equal to 5.0% of the Series A Preferred Stock liquidation preference per year, which dividend may be paid in cash or added to the Series A Preferred Stock liquidation preference;
- each share of Series A Preferred Stock has an initial liquidation preference of $100 and the liquidation preference accretes daily at an annual rate of 5.0%, compounded semi-annually;

Table of Contents

- upon a change of control of our company, Warburg Pincus may elect to (i) convert the shares of Series A Preferred Stock into shares of Common Stock and receive the consideration due to the holders of Common Stock upon conversion, or (ii) cause us to redeem the Series A Preferred Stock for cash at the liquidation preference then in effect;
- if a change of control occurs within 5 years of the issuance of the Series A Preferred Stock, the liquidation preference shall be an amount equal to the liquidation preference then in effect plus a premium of (i) 15% if the change of control occurs prior to the first anniversary of the issuance of the Series A Preferred Stock, (ii) 10% if the change of control occurs after the first anniversary of the issuance of the Series A Preferred Stock but prior to the second anniversary of the issuance of the Series A Preferred Stock, (iii) 5% if the change of control occurs after the second anniversary of the issuance of the Series A Preferred Stock but prior to the fourth anniversary of the issuance of the Series A Preferred Stock or (iv) 1% if the change of control occurs after the fourth anniversary of the issuance of the Series A Preferred Stock but prior to the fifth anniversary of the issuance of the Series A Preferred Stock;
- holders of Series A Preferred Stock have rights to acquire additional shares of our capital stock or rights to purchase property in the event of certain grants, issuances or sales;
- the conversion price of the Series A Preferred Stock, which initially was $13.51 per share, is subject to customary broad-based weighted average anti-dilution adjustments and other customary adjustments upon the issuance of shares of Common Stock below the conversion price, such as the issuance of shares and options to purchase shares in the CipherTrust acquisition, which resulted in an adjustment to the conversion price of the Series A Preferred Stock to $12.75;
- the approval of holders of majority of the Series A Preferred Stock is separately required to (i) approve changes to our certificate of incorporation or bylaws that adversely affect Warburg Pincus's rights, (ii) adopt any stockholder rights plan that would dilute the economic or voting interest of Warburg Pincus, (iii) incur certain debt, distribute assets, pay dividends or repurchase securities, (iv) create or issue any equity security with rights senior to or on parity with the Series A Preferred Stock, (v) increase the size of our board of directors above nine members and (vi) take any action that adversely affects the rights, preferences and privileges of the Series A Preferred Stock; and
- for so long as Warburg Pincus and its affiliates owns at least 50% of its shares of Series A Preferred Stock, the holders of Series A Preferred Stock will have the right, voting as a separate class, to appoint one member to our board of directors.

The potential increase in sales from our relationships with various vendors of communications, security, and network management products or managed services may be reduced by requirements to provide volume price discounts and other allowances and significant costs incurred in customizing our products. Although we do not intend that such relationships be exclusive, we may be required to enter into an exclusive relationship or forego a significant sales opportunity. To the extent we become dependent on actions by such parties, we could be adversely affected if the parties fail to perform as expected. To minimize our risk, we often set minimum quotas with our customers as a condition of exclusivity.

Competition from companies producing enterprise gateway security products could reduce our sales and market share. The market for enterprise gateway security products is intensely competitive and characterized by rapid technological change. We believe that competition in this market is likely to persist and to intensify as a result of increasing demand for security products. Each of our individual products competes with a different group of competitors and products. Because the market for our products is highly competitive, it may be difficult to significantly increase our market share or our market share may actually decline.

Our customers' purchasing decisions are based heavily upon the quality of the security our products provide, the ease of installation and management, the ability to increase the numbers of individuals using our software simultaneously, and the flexibility of our software. If a competitor can offer our customers a better solution in these areas or others and we are unable to rapidly offer a competitive product, we may lose customers. Competitors with greater resources could offer new solutions rapidly and at relatively low costs which could lead to increased price pressure, reduced margins, and a loss of market share.

Many of our competitors and potential competitors have significantly greater financial, marketing, technical, and other competitive resources than we have. Our larger actual and potential competitors may be able to leverage an installed customer base and/or other existing or future enterprise-wide products, adapt more quickly to new or emerging technologies and changes in customer requirements, or devote greater resources to the promotion and sale of their products than we can. Additionally, we may lose product sales to these competitors because of their greater name recognition and reputation among potential customers.

Our future potential competitors could include developers of operating systems or hardware suppliers not currently offering competitive enterprise gateway security products, including Microsoft, Sun Microsystems, Inc., IBM, Computer Associates, and Hewlett Packard. If any of those potential competitors begins to offer enterprise-wide security systems as a component of its hardware, demand for our solutions could decrease. Ultimately, approaches other than ours may dominate the market for enterprise gateway security products.

In the future, we may also face competition from our competitors and other parties that develop or acquire enterprise gateway security products based upon approaches that we employ. There are no guarantees that our approach will dominate the market for enterprise gateway security products. While we believe that we do not compete against manufacturers of other classes of security products, such as encryption, due to the complementary functions performed by such other classes, our customers may perceive such other companies as our competitors.

Consolidation among competitors may erode our market share. Current and potential competitors have established, or may in the future establish, cooperative relationships among themselves or with third parties to increase the ability of their products to address the needs of our prospective customers. Accordingly, it is possible that new competitors or alliances may emerge and rapidly acquire significant market share. If this were to occur, it could materially and adversely affect our financial condition or results of operations.

The trend toward multi-function security solutions may result in a consolidation of the market around a smaller number of vendors that are able to provide the necessary breadth of products and services. In the event that we are unable to internally develop all of the products needed for a complete, secure e-business solution, we may need to acquire such technology or be acquired by a larger entity. However, there can be no assurance that, in the event that we are not able to internally develop all of the products needed for an enterprise-wide security solution, we will be able to acquire or merge with other entities on terms favorable to us and our stockholders.

The pricing policies of our competitors may impact the overall demand for our products and services and therefore, impacting our profitability. Some of our competitors are capable of operating at significant losses for extended periods of time, enabling them to sell their products and services at a lower price. If we do not maintain competitive pricing, the demand for our products and/or services, as well as our market share, may decline, having an adverse effect on our business. From time to time, in responding to competitive pressures we lower the price of our products and services. When this happens, if we are unable to reduce our component costs or improve operating efficiencies, our margins could be adversely affected.

Other vendors may include products similar to ours in their hardware or software and render our products obsolete. In the future, vendors of hardware and of operating systems or other software may continue to enhance their products or bundle separate products to include functions that are currently provided primarily by enterprise gateway security software. If network security functions become standard features of computer hardware or of operating system software or other software, our products may become obsolete and unmarketable, particularly if the quality of these security features is comparable to that of our products. Furthermore, even if the enterprise gateway security and/or management functions provided as standard features

Table of Contents

by hardware providers or operating systems or other software is more limited than that of our products, our customers might accept this limited functionality in lieu of purchasing additional software. Sales of our products would suffer materially if we were then unable to develop new enterprise gateway security and management products to further enhance operating systems or other software and to replace any obsolete products.

If an OEM customer reduces or delays purchases, our revenue may decline and/or our business could be adversely affected. We currently have formed relationships with several OEMs including Cisco, Blue Coat, McAfee, Computer Associates, F5 Networks, Inc. and Network Appliance. If we fail to sell to such OEMs in the quantities expected, or if any OEM terminates our relationship, this could adversely affect our reputation, the perception of our products and technology in the marketplace and the growth of our business, and your investment in our common stock may decline in value.

Technology in the enterprise gateway security market is changing rapidly, and if we fail to develop new products that are well accepted, our market share will erode. To compete successfully, we must enhance our existing products and develop and introduce new products in a timely manner. Our net sales and operating results could be materially affected if we fail to introduce new products on a timely basis. The rate of new enterprise gateway security product introductions is substantial and security products have relatively short product life cycles. Our customer requirements and preferences change rapidly. Our net sales and operating results will be materially affected if the market adopts, as industry standards, solutions other than those we employ.

Denial of our patent applications or invalidation or circumvention of our patents may weaken our ability to compete in the enterprise gateway security market. While we believe that our pending applications relate to patentable devices or concepts, there can be no assurances that any pending or future patent applications will be granted. There is also the risk that a current or future patent, regardless of whether we are an owner or a licensee of such patent, may be challenged, invalidated or circumvented. In addition, there are no assurances that the rights granted under a patent or under licensing agreements will provide competitive advantages to us.

If another party alleges that we infringe its patents or proprietary rights, we may incur substantial litigation costs. Other than a claim made by Finjan Software Ltd., we are not aware of any third party claims that we or our products have infringed a patent or other proprietary rights. However, the computer technology market is characterized by frequent and substantial intellectual property litigation. Intellectual property litigation is complex and expensive, and the outcome of such litigation is difficult to predict. In the event that a third party were to make a claim of infringement against us, we could be required to devote substantial resources and management time to the defense of such claim, which could have a material adverse effect on our business and results of operations.

Disclosure of our trade secrets or proprietary information may undermine our competitive advantages. There can be no assurances that the confidentiality agreements protecting our trade secrets and proprietary expertise will not be breached, that we will have adequate remedies for any breach, or that our trade secrets will not otherwise become known to or independently developed by competitors.

If the use of public switched networks such as the Internet does not continue to grow, our market and ability to sell our products and services may be limited. Our sales also depend upon a robust industry and infrastructure for providing access to public switched networks, such as the Internet. If the infrastructure or complementary products necessary to take these networks into viable commercial marketplaces are not developed or, if developed, these networks do not become and continue to be viable commercial marketplaces, our net sales and operating results could suffer.

Our reliance on third party manufacturers of hardware components and subassemblies that are used in our appliances and SafeWord token product lines could cause a delay in our ability to fill orders. We currently purchase the hardware components for our appliance and Safeword token product lines from several major suppliers. Delays in receiving components would harm our ability to deliver our products on a timely basis and net sales and operating results could suffer.

Our product lines are not diversified beyond providing enterprise gateway security solutions to our customers, and any drop in the demand for enterprise gateway security products would materially harm our business. Substantially all of our revenue comes from sales of enterprise gateway security products and related services. We expect this will continue for the foreseeable future. As a result, if for any reason our sales of these products and services are impeded, our net sales and operating results will be significantly reduced.

Our stock price is highly volatile, which may cause our investors to lose money and may impair our ability to raise money, if necessary. The price of our common stock, like that of many technology companies, has fluctuated widely. During 2006, our stock price ranged from a per share high of $15.29 to a low of $4.82. Fluctuation in our stock price may cause our investors to lose money and impair our ability to raise additional capital, if necessary. Factors that may affect stock price volatility include:

- Unexpected fluctuations in operating results;
- Our competitors or us announcing technological innovations or new products;
- General economic conditions and weaknesses in geographic regions of the world;
- Threat of terrorist attacks or acts of war in the U.S. or abroad;
- Developments with respect to our patents or other proprietary rights or those of our competitors;
- Our ability to successfully execute our business plan and compete in the enterprise gateway security industry;
- Relatively low trading volume;
- Product failures; and
- Analyst reports and media stories.

If our products fail to function properly or are not properly designed, our reputation may be harmed, and customers may make product liability and warranty claims against us. Our customers rely on our enterprise gateway security products to prevent unauthorized access to their networks and data transmissions. These customers include major financial institutions, defense-related government agencies protecting national security information, and other large organizations. These customers use our products to protect confidential business information with commercial value far in excess of our net worth. Therefore, if our products malfunction or are not properly designed, we could face warranty and other legal claims, which may exceed our ability to pay. We seek to reduce the risk of these losses by attempting to negotiate warranty disclaimers and liability limitation clauses in our sales agreements. However, these measures may ultimately prove ineffective in limiting our liability for damages.

In addition to any monetary liability for the failure of our products, an actual or perceived breach of network or data security at one of our customers could harm the market's perception of our products and our business. The harm could occur regardless of whether that breach is attributable to our products.

We also face the more general risk of bugs and other errors in our software. Software products often contain undetected errors or bugs when first introduced or as new versions are released, and software products or media may contain undetected viruses. Errors or bugs may also be present in software that we license from third parties and incorporate into our products. Errors, bugs, or viruses in our products may result in loss of or delay in market acceptance, recalls of hardware products incorporating the software, or loss of data. Our net sales and operating results could be materially reduced if we experience delays or difficulties with new product introductions or product enhancements.

If we lose a significant customer, we will realize smaller profits. We derive a significant portion of our revenues from a limited number of customers. For example, our top five customers made up 10% of our sales in 2006. If we lose any of these customers or if our revenues from any of these customers are reduced, and we fail to replace the customer or fail to increase sales from other customers, we will incur smaller profits.

If we fail to collect amounts due from our customers on a timely basis, our cash flow and operating results may suffer. Because the timing of our revenues is difficult to predict and our expenses are often difficult to reduce in the short run, management of our cash flow is very important to us. Like most companies, we anticipate that a portion of the amounts owed to us will never be paid. However, if our actual collection of amounts owed to us is less than we have estimated, we will have less cash to fund our operations than we anticipated, and our financial condition and operating results could be adversely affected.

In addition, collection of amounts due us from sales to international customers generally takes longer than for other sales. Therefore, if our sales to international customers increase as a percentage of our total revenue, the average number of days it takes for us to collect amounts due from our customers may increase. If there is an increase in the time required for us to collect amounts due us, we will have less cash to fund our operations than we anticipated. This in turn could adversely affect our financial condition and operating results.

We have taken and may from time to time take various forms of action to manage the amounts due us from customers and grant customer discounts in exchange for earlier payment.

Quarterly net sales and operating results depend on the volume and timing of orders received, which may be affected by large individual transactions and which sometimes are difficult to predict. Our quarterly operating results may vary significantly depending on a number of other factors, including:

- The timing of the introduction or enhancement of products by us or our competitors;
- The size, timing, and shipment of individual orders;
- Market acceptance of new products;
- Changes in our operating expenses;
- Personnel departures and new hires and the rate at which new personnel become productive;
- Mix of products sold;
- Changes in product pricing;
- Development of our direct and indirect distribution channels;
- Costs incurred when anticipated sales do not occur; and
- General economic conditions.

Sales of our products generally involve a significant commitment of capital by customers, with the attendant delays frequently associated with large capital expenditures. For these and other reasons, the sales cycle for our products is typically lengthy and subject to a number of significant risks over which we have little or no control. We are often required to ship products shortly after we receive orders, and consequently, order backlog, if any, at the beginning of any period has in the past represented only a small portion, if any, of that period's expected revenue. As a result, our product sales in any period substantially depends on orders booked and shipped in that period. We typically plan our production and inventory levels based on internal forecasts of customer demand, which are highly unpredictable and can fluctuate substantially.

If customer demand falls below anticipated levels, it could seriously harm our operating results. In addition, our operating expenses are based on anticipated revenue levels, and a high percentage of our expenses are generally fixed in the short term. Based on these factors, a small fluctuation in the timing of sales can cause operating results to vary significantly from period to period.

The Internet may become subject to increased regulation by government agencies. Due to the increasing popularity and use of the Internet, it is possible that a number of laws and regulations may be adopted with respect to the Internet, covering issues such as user privacy, pricing and characteristics, and quality of products

Table of Contents

and services. In addition, the adoption of laws or regulations may slow the growth of the Internet, which could in turn decrease the demand for our products and increase our cost of doing business or otherwise have an adverse effect on our business, operating results or financial condition.

Anti-takeover provisions in our charter documents, share rights agreement, and Delaware law could discourage a takeover or future financing. The terms of our certificate of incorporation and share rights agreement permit our Board of Directors to issue up to 2,000,000 shares of preferred stock and determine the price, rights, preferences, privileges, and restrictions, including voting rights, of those shares without any further vote or action by our stockholders.

The Board may authorize the issuance of additional preferred stock with voting or conversion rights that could materially weaken the voting power or other rights of the holders of our common stock. The issuance of preferred stock, while providing desirable flexibility in connection with possible acquisitions and other corporate purposes could make it more difficult for a third party to acquire a majority of our outstanding voting stock. Further, provisions of Delaware law, our certificate of incorporation and our bylaws, such as a classified board and limitations on the ability of stockholders to call special meetings, and provisions of our share rights agreement could delay or make more difficult a merger, tender offer, proxy contest, or other takeover attempts.

The ability to attract and retain highly qualified personnel to develop our products and manage our business is extremely important, and our failure to do so could harm our business. We believe our success depends to a large extent upon a number of key technical and management employees. We may be unable to achieve our sales and operating performance objectives unless we can attract and retain technically qualified and highly skilled engineers and sales, consulting, technical, financial, operations, marketing, and management personnel. These personnel are particularly important to our research and development efforts and, as such, we employ a large number of technical personnel holding advanced degrees and special professional certification. Competition for qualified personnel is intense, and we expect it to remain so for the foreseeable future. We may not be successful in retaining our existing key personnel and in attracting and retaining the personnel we require. Our operating results and our ability to successfully execute our business plan will be adversely affected if we fail to retain and increase our key employee population.

Our international operations subject us to risks related to doing business in foreign countries. International sales are a substantial portion of our business. Although all of our sales are payable in U.S. dollars as of December 31, 2006, several factors could make it difficult for customers from foreign countries to purchase our products and services or pay us for obligations already incurred. Such factors include:

- Severe economic decline in one of our major foreign markets; and
- Substantial decline in the exchange rate for foreign currencies with respect to the U.S. dollar.

A decline in our international sales or collections of amounts due us from customers could materially affect our operations and financial conditions. For fiscal year 2006, 39% of our total revenue came from international sales compared to 38% in 2005. A very large drop in our sales or collections of amounts due us in these specific countries as a result of recession or other economic or political disturbances would likely harm our net sales and operating results.

In addition, we face a number of general risks inherent in doing business in international markets including, among others:

- Unexpected changes in regulatory requirements;
- Tariffs and other trade barriers;
- Legal uncertainty regarding liability;
- Threat of terrorist attacks or acts of war;

Table of Contents

- Political instability;
- Potentially greater difficulty in collecting amounts due us;
- Longer periods of time to collect amounts due us; and
- A higher rate of piracy of our products in countries with a high incidence of software piracy.

ITEM 2. PROPERTIES

We are currently headquartered in 10,895 square feet of office space in San Jose, California. We have a facility in St. Paul, Minnesota with 107,344 square feet occupied by production, research and development, customer support and administration. We have a facility in Alpharetta, Georgia with a square footage of 75,288 that is occupied by research and development, customer support and sales. We have research facilities located in Concord, California and Deerfield Beach, Florida that occupy 17,240 and 30,148 square feet, respectively. We have foreign research facilities located in Woolongabong, Australia and Paderborn, Germany that occupy 9,529 square feet and 11,006 square feet, respectively. In support of our U.S. field sales organization, we also lease 8,198 square feet of office space in Reston, Virginia, and 10,102 in Seattle, Washington. We terminated our operations at the Seattle, Washington facility during the first quarter of 2007 but expect to sublease the facility in the future. We occupy these premises under leases expiring at various times through the year 2016. We also have foreign offices in London, England; Sydney, Australia; Munich, Germany; Paris, France; Singapore; Japan; Dubai; China and Hong Kong. We believe that our facilities are adequate for our current needs.

ITEM 3. LEGAL PROCEEDINGS

On June 5, 2006, Finjan Software, Ltd. filed a complaint entitled Finjan Software, Ltd. v. Secure Computing Corporation in the United States District Court for the District of Delaware against Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG. The complaint alleges that Secure Computing and its named subsidiaries infringe U.S. Patent No. 6,092,194 ("'194 Patent") based on the manufacture, use, and sale of the Webwasher Secure Content Management suite. Secure Computing denies infringing any valid claims of the '194 Patent. The answer to the complaint was filed on July 26, 2006. Discovery is proceeding.

On January 19, 2007, Rosenbaum Capital, LLC filed a putative securities class action complaint in the United States District Court for the Northern District of California against us and certain directors and officers of the company. The alleged plaintiff class includes persons who acquired our stock between May 4, 2006 through July 11, 2006. The complaint alleges generally that defendants made false and misleading statements about our business condition and prospects for the fiscal quarter ended June 30, 2006, in violation of Section 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. The complaint seeks unspecified monetary damages. While there can be no assurance as to the outcome of this or any other litigation we believe there are meritorious legal and factual defenses to this action and we intend to defend ourselves vigorously.

ITEM 4. SUBMISSION OF MATTERS TO A VOTE OF SECURITY HOLDERS

No matters were submitted to a vote of the stockholders during the three months ended December 31, 2006.

Table of Contents

PART II

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information

Our common stock is listed on the NASDAQ national market under ticker symbol: SCUR. As of March 12, 2007, there were approximately 3,900 registered holders. The number of registered holders represents the number of shareholders of record plus the number of individual participants in security position listings. We believe, however, that many beneficial holders of our common stock have registered their shares in nominee or street name and that there are approximately 14,000 beneficial owners. The low and high sale price of our common stock during the last eight quarters is as follows:

	2006		2005	
Quarter	High	Low	High	Low
First	15.29	11.08	10.75	7.38
Second	11.85	7.65	11.83	8.01
Third	8.68	4.82	12.91	10.32
Fourth	7.27	6.15	14.70	10.74

We have not paid any dividends on our common stock during the periods set forth above. It is presently the policy of the Board of Directors to retain earnings for use in expanding and developing our business. Accordingly, we do not anticipate paying dividends on the common stock in the foreseeable future.

Sale of Unregistered Securities

On August 17, 2005, we entered into a Securities Purchase Agreement with Warburg Pincus IX, L.P., as amended December 9, 2005. Pursuant to the terms of the Securities Agreement, we agreed to issue to Warburg Pincus 700,000 shares of Series A Preferred Stock and a warrant to purchase 1,000,000 shares of our common stock in exchange for $70 million, subject to stockholder approval, among other conditions. The shares of Series A Preferred Stock are convertible at $12.75 a share, and include a 5% accretive dividend. The warrant is exercisable at a price of $13.85 per share. On January 11, 2006, our stockholders approved the issuance of shares of Series A Preferred Stock and a warrant to purchase shares of our common stock to Warburg Pincus, and we issued the shares of Series A Preferred Stock and the warrant on January 12, 2006. The issuance was deemed to be exempt from registration under the Securities Act of 1933 in reliance upon Section 4(2) thereof as transactions by an issuer not involving any public offering. We filed a Registration Statement on Form S-3 which registered the shares of common stock issuable upon conversion of the Series A Preferred Stock and the common stock issuable upon exercise of the warrant for resale.

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. The aggregate purchase price was $270.1 million consisting primarily of $188.1 million in cash, the issuance of 10.0 million shares of common stock valued at $68.1 million, the conversion of outstanding CipherTrust stock options into options to purchase 2.5 million shares of our common stock with a fair value of $7.8 million, and direct costs of the acquisition of $6.1 million. The issuance of 10.0 million shares of common stock was exempt from registration pursuant to Section 4(2) of the Securities Act of 1933, as amended, and pursuant to Rule 506 of Regulation D of the Securities Act.

Table of Contents

Performance Evaluation

The graph below compares total cumulative stockholders' return on the common stock for the period from the close of the NASDAQ Stock Market—U.S. Companies on December 31, 2001 to December 31, 2006, with the total cumulative return on the Computer Index for the NASDAQ Stock Market—U.S. Companies (the "Computer Index") and the Composite Index for the NASDAQ Stock Market (the "Composite Index") over the same period. The index level for the graph and table was set to 100 on December 31, 2001 for the common stock, the Computer Index and the Composite Index and assumes the reinvestment of all dividends.

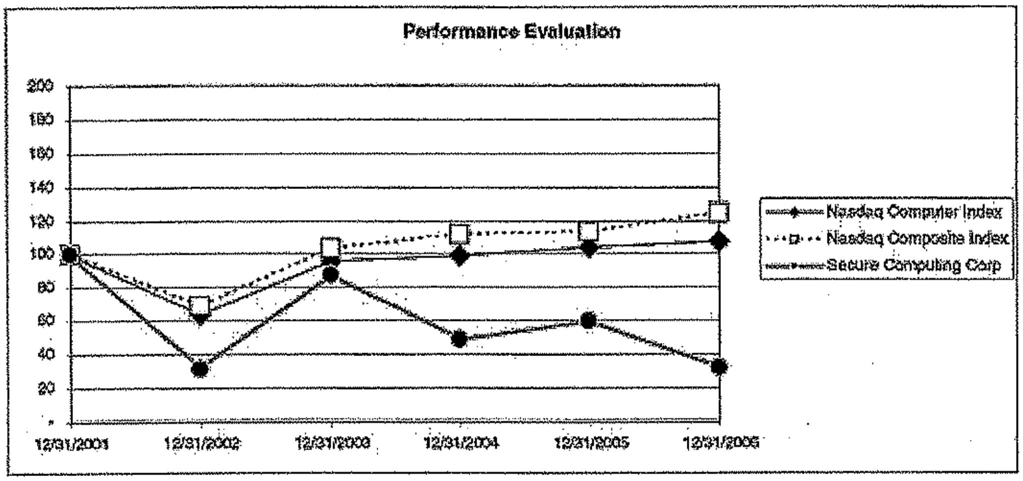


Table of Contents

ITEM 6. SELECTED FINANCIAL DATA

The consolidated statement of operations data set forth below for the fiscal years ended December 31, 2006, 2005 and 2004, and the consolidated balance sheet data at December 31, 2006 and 2005, are derived from the audited consolidated financial statements included elsewhere in this Form 10-K. The consolidated statement of operations data set forth below for the fiscal years ended December 31, 2003 and 2002 and the consolidated balance sheet data at December 31, 2004, 2003 and 2002, are derived from audited consolidated financial statements which are not included in this Form 10-K. You should read the data set forth below in conjunction with the financial statements and notes thereto and "Management's Discussion and Analysis of Financial Condition and Results of Operations" included elsewhere in this Form 10-K.

	Year Ended December 31,				
	(Table in thousands, except per share amounts)				
	2006	2005	2004	2003	2002
STATEMENT OF OPERATIONS DATA:					
Revenue	$176,697	$109,175	$ 93,378	$ 76,213	$61,960
Gross profit	127,539	87,126	75,991	63,578	51,654
Net (loss) income from continuing operations	(27,398)	21,374	12,835	9,290	(5,166)
Net loss from discontinued operations/disposal of AT division	—	—	—	(1,034)	(1,310)
Net (loss) income	(27,398)	21,374	12,835	8,256	(6,476)
Net (loss) income applicable to common shareholders	(43,551)	21,374	12,835	8,256	(6,476)
Basic (loss) income per share:					
Continuing operations	(0.76)	0.59	0.36	0.29	(0.18)
Discontinued operations	—	—	—	(0.03)	(0.04)
Basic (loss) income per share	$ (0.76)	$ 0.59	$ 0.36	$ 0.26	$ (0.22)
Diluted (loss) income per share:					
Continuing operations	(0.76)	0.57	0.34	0.28	(0.18)
Discontinued operations	—	—	—	(0.03)	(0.04)
Diluted (loss) income per share	$ (0.76)	$ 0.57	$ 0.34	$ 0.25	$ (0.22)
BALANCE SHEET DATA:					
Total assets (1)	724,128	171,763	130,914	108,475	60,943
Debt, net of fees	85,023	—	—	—	—
Convertible preferred stock	65,558	—	—	—	—
Stockholders' equity	409,741	121,883	91,826	72,014	29,663

(1) Total assets include goodwill from acquisitions of $533.7 million for 2006, $39.2 million for 2005, $39.3 million for 2004, $40.5 million for 2003, and $15.2 million for 2002.

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

Information Regarding Forward-Looking Statements

The following discussion contains forward-looking statements, including statements regarding our expectations, beliefs, intentions, or strategies regarding the future. These statements are not guarantees of future performance and are subject to risks, uncertainties, and other factors, some of which are beyond our control and difficult to predict and could cause actual results to differ materially from those expressed or forecasted in the forward-looking statements. The risks and uncertainties are summarized in Item 1A above and in the other documents we file with the SEC. These forward-looking statements reflect our view only as of the date of this report. We cannot guarantee future results, levels of activity, performance, or achievement. We do not undertake any obligation to update or correct any forward-looking statements.

Table of Contents

Executive Overview

We are a leading provider of enterprise gateway security solutions. Our best-of-breed portfolio of solutions provides Web Gateway, Messaging Gateway, and Network Gateway security, as well as Identity and Access Management that are further differentiated by the proactive protection provided by TrustedSource (global intelligence).

Our specialized solutions are designed to meet customers' needs to balance security and accessibility, and to help them create trusted environments both inside and outside their organizations. Each of our products provides a complete solution in and of itself, and they also integrate with each other for a more comprehensive, unified, and centrally managed solution. We have developed a vision for comprehensive security on the enterprise gateway that embodies the following core design principles: appliance-based delivery; application and content awareness; centralized policy, management and reporting; bi-directional protection; proactive protection; user management and education; performance; and resiliency.

In 2005 we embarked on a strategy to significantly increase our presence in the industry and to define and become the leader in the enterprise gateway security market. We believe that our acquisitions of CyberGuard and CipherTrust in 2006 have laid a strong foundation for our future success.

Through the CipherTrust acquisition in 2006, we acquired TrustedSource technology and entered the Messaging Gateway security market. We believe TrustedSource technology is the most precise and comprehensive Internet host reputation system in the world, and we are rolling this system into many of our product lines as a key cornerstone of Global Intelligence security. Recognizing that messaging is now a primary business application in most enterprises, we have implemented a strategy to comprehensively address both inbound and outbound threats and to help our customers insure compliance with federally mandated requirements for the protection of sensitive data. Our Messaging Gateway Security products include IronMail, IronIM, RADAR, and Secure Computing Edge.

Also in 2006, we added the Webwasher Web Gateway security product to our Web Security Gateway product line through the CyberGuard acquisition. Web Gateway Security appliances protect enterprises from malware, data leakage, and Internet misuse, while helping to ensure policy enforcement, regulatory compliance, and a productive application environment.

This year we continued to differentiate our UTM appliance from the competition with demonstrable zero-hour attack protections on high profile Internet attacks (such as the Sendmail vulnerability in March and Microsoft Windows MetaFile "WMF" attack in January). We also announced plans to merge our newly-acquired CyberGuard Firewall/VPN technologies (TSP and Classic) with our Sidewinder G2 Security Appliance in our next generation UTM appliance that has come to market in the first quarter of 2007. The CyberGuard acquisition also brought to us a new paradigm in enterprise central management with the Command Center which we will continue to leverage going forward. We believe Command Center's ability to do administration, configuration, monitoring, and management of software updates for a global appliance deployment coupled with our Security Reporter product's central reporting, and full out-of-the box compliance reports, continue to ensure that both medium and large customers see our network gateway appliances as the product of choice.

Early in 2006 we broadened our presence in the authentication market into the IAM space by introducing our SafeWord SecureWire appliance. SafeWord SecureWire is a new, robust technology that functions as the access, authentication, and compliance hub for the entire network. By providing secure access management inside and outside the virtual perimeter, and by consolidating all policies on a single device, SecureWire helps enable our customers to achieve configuration compliance because only properly configured devices are allowed to access their networks.

Our Network Gateway Security revenue represented 53% of total revenue and an 87% or $43.3 million increase over the prior year. The acquired CyberGuard TSP and Classic product lines contributed $44.7 million.

Our Web Gateway Security revenue represented 26% of total revenue and a 46% or $14.6 million increase over the prior year. The acquired Webwasher product line contributed $18.4 million. This increase was slightly offset by a $3.5 million decline in sales of our Bess and Sentian product lines when these products were discontinued in 2006. Our Identity and Access Management revenue represented 17% of total revenue, which is a 9% increase over the prior year. This increase was driven by sustained demand for high assurance solutions. Messaging Gateway Security revenue, added through the sales of the acquired CipherTrust product line, represented 4% of total revenue for the full year 2006. Because we are unable to establish vendor specific objective evidence (VSOE) of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred and will be recognized as revenue over the term of the undelivered elements.

Our customers operate some of the largest and most sensitive networks and applications in the world. Our partners and customers include the majority of the Dow Jones Global 50 Titans and numerous organizations in the Fortune 1000, as well as banking, financial services, healthcare, telecommunications, manufacturing, public utilities, schools and federal, state and local governments. We also have close relationships with the largest agencies in the U.S. government.

International sales accounted for 39% of total revenue during 2006. Major foreign markets for our products include Europe, Japan, China, the Pacific Rim and Latin America. In each market, we have independent channel partners responsible for marketing, selling and supporting our products to resellers and end users. In 2006, our market presence continued to expand through our extensive worldwide network of value-added resellers, distributors, and OEM partners. These partners generated 81% of our sales in 2006.

Each of our individual products competes with a different group of competitors and products. In this highly competitive market, characterized by rapid technological change, our customers' purchasing decisions are based heavily upon the quality of the security our products provide, the ease of installation and management, and the scalability and flexibility of our software.

Specific challenges and risks that our product lines face include, but are not limited to: responding to competitor pricing policies and competitive features; rapid technological change in the network security market; and risk of bugs and other errors in our software.

On January 11, 2006, we completed our acquisition of CyberGuard Corporation, a leading provider of network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication, in a stock and cash transaction valued at $310.7 million. This acquisition strengthened our position as one of the market leaders in Network Gateway Security appliances, and strengthened our position in the Web Gateway Security space. CyberGuard was a logical fit for Secure Computing, enhancing our strategic vision and better positioning us in two rapidly growing segments of the security industry. Along with an expanded customer and partner base, this merger provided us with important competitive advantages in the Network and Web Gateway Security markets.

On January 12, 2006, we received from Warburg Pincus Private Equity IX, L.P., a global private equity fund, $70.0 million in proceeds from the issuance of 700,000 of Series A Convertible Preferred Stock (the preferred stock), a warrant to acquire 1.0 million shares of our common stock that vested on that date and an election of a member to our Board of Directors. Based on a quoted market price as of January 12, 2006 and the fair value of the warrant as determined using the Black-Scholes model, we valued the preferred stock at $62.0 million and the warrant at $8.0 million. The proceeds from this transaction were used to finance most of the cash portion of the CyberGuard acquisition. On August 31, 2006, the conversion price for the preferred stock was adjusted from the original price of $13.51 to $12.75 per share and the exercise price for the warrant was adjusted from the original price of $14.74 to $13.85 per share in accordance with an anti-dilution provision triggered by the CipherTrust acquisition.

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. The CipherTrust products provide innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. The acquired products from CipherTrust include IronMail, powered by TrustedSource, IronIM, IronMail Edge, IronNet, and RADAR. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and Messaging Gateway security needs.

On August 31, 2006, we entered into a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank. The credit facility provided for a $90.0 million term loan facility, a $20.0 million revolving credit facility, and a swingline loan sub-facility. The proceeds from this transaction were used to finance a portion of the CipherTrust acquisition. The term loan matures on August 31, 2013 and is payable in 27 scheduled quarterly installments of $225,000 beginning in December 2006 with a final payment of $83.9 million due at maturity. Interest is payable quarterly on the term loan at the London Interbank Offered Rate ("LIBOR") + 3.25%. The interest rate on the term loan may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +3.00%.

The revolving credit facility matures on August 31, 2012 with interest payable quarterly at LIBOR + 3.25%. The interest rate on the revolving credit facilities may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +2.75%. The revolving credit facility also requires that we pay an annual commitment fee of .5%. The annual commitment fee, based on our Leverage Ratio and ranging from .5% to .375%, is payable quarterly in arrears. The Leverage Ratio is defined as the ratio of (a) consolidated indebtedness to (b) consolidated adjusted EBITDA (earnings before interest, taxes, depreciation, amortization and other adjustments as defined in the agreement). The Leverage Ratio will be calculated quarterly on a pro forma basis that includes the four preceding quarters. The initial Leverage Ratio calculation will be as of December 31, 2006 and cannot exceed the following thresholds over the term of the loan: August 31, 2006 through December 31, 2006 – 4.75 to 1.00; First six months of Fiscal 2007 – 4.00 to 1.00; Last six months of Fiscal 2007 – 3.50 to 1.00; Fiscal 2008 – 2.50 to 1.0; Fiscal 2009 – 2.25 to 1.00; Fiscal 2010 through maturity – 2.00 to 1.00.

The obligations under the senior secured credit facility are guaranteed by us and are secured by a perfected security interest in substantially all of our assets. Financing fees incurred in connection with the credit facility were deferred and are included as a reduction to our long-term debt. These fees are being amortized to interest expense over the term of the term loan using the effective interest rate method.

The credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain financial covenants, including maintaining leverage and interest coverage ratios and capital expenditure limitations.

We incurred a net loss $27.4 million in 2006 compared to net income of $21.3 million in 2005. The net loss is a result of costs not incurred in 2005, such as: share-based compensation of $10.6 million, litigation expense of $2.5 million, amortization of intangible assets of $16.5 million, additional tax expense of $8.9 million and one-time acquisition related costs and write-off of impaired fixed asset of $2.6 million. In addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates. Until we are able to establish VSOE on the sales of our CipherTrust product line and our revenue outpaces our operating expenses, including share-based compensation and amortization of intangible assets, we expect to generate net losses going forward.

As of December 31, 2006, we had $8.7 million in cash and short-term investments with no outstanding borrowings on our $20 million revolving credit facility. We generated $36.1 million in cash from operations for the year. We expect to generate cash during 2007 as we expect billings to continue to grow at a faster rate than operating expenses.

Table of Contents

Results of Operations

The following table sets forth, for the periods indicated, the statements of operations of our company expressed as a percentage of revenue:

	Year ended December 31,		
	2006	2005	2004
Revenues:			
Products	65%	73%	72%
Services	35	27	28
Total revenues	100	100	100
Cost of revenues:			
Products	18	15	13
Services	7	5	6
Amortization of purchased intangibles	3	—	—
Total cost of revenues	28	20	19
Gross profit	72	80	81
Operating expenses:			
Selling and marketing	48	39	44
Research and development	19	15	17
General and administrative	8	7	7
Amortization of purchased intangibles	6	—	—
Litigation settlement	1	—	—
Total operating expenses	82	61	68
Operating (loss)/income	(10)	19	13
Other (expense)/income	(—)	2	1
(Loss)/income before tax	(10)	21	14
Income tax expense	(6)	(1)	—
Net (loss)/income	(16%)	20%	14%
Preferred stock accretion	(2)	—	—
Charge from beneficial conversion of preferred stock	(7)	—	—
Net (loss)/income applicable to common shareholders	(25%)	20%	14%

Comparison of Years Ended December 31, 2006 and 2005.

Revenue. Our total revenues increased 62% to $176.7 million in 2006, up from $109.2 million in 2005. Our product revenues increased 46% to $115.6 million in 2006, up from $79.3 million in 2005. Our service revenues increased 105% to $61.1 million in 2006, up from $29.8 million in 2005. The increase in total revenues in 2006 was driven by growth across all product categories. Our Network Gateway Security revenue represented 53% of total revenue and an 87% or $43.3 million increase over the prior year. The acquired CyberGuard TSP and Classic product lines contributed $44.7 million. Our Web Gateway Security revenue represented 26% of total revenue and a 46% or $14.6 million increase over the prior year. The acquired Webwasher product line contributed $18.4 million. This increase was slightly offset by a $3.5 million decline in sales of our Bess and Sentian products when these products were discontinued in 2006. Our Identity and Access Management revenue represented 17% of total revenue, which is a 9% increase over the prior year. This increase was driven by sustained demand for high assurance solutions. Messaging Gateway Security revenue, added through the sales of the acquired CipherTrust product lines and represented 4% of total revenue for the full year 2006. Because we are unable to establish

VSOE of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred and will be recognized as revenue over the term of the undelivered elements.

Table of Contents

Cost of Revenues and Gross Profit. Total cost of revenues, which includes products and services costs and the amortization of purchased intangibles, increased 124% to $49.2 million in 2006, up from $22.0 million in 2005. This increase is the direct result of the increase in total revenues and the addition of the amortization of purchased intangibles and share-based compensation. Gross profit as a percentage of revenue decreased from 80% in 2005 to 72% in 2006. Gross profit for products decreased to 68% in 2006 compared to 79% in 2005. This decline was driven by the amortization of the developed technologies acquired in the CyberGuard and CipherTrust acquisitions and by the increased sales volume on products containing a hardware component, which have a lower gross profit margin than our software products. Gross margins were also reduced as more of our business continues to be transacted with channel partners versus direct to end users. In 2006 sales to our indirect channel partners comprised 81% of total sales versus 73% of total sales in 2005. Gross profit for services was 81% in 2006 compared to 83% in 2005. The decline in the gross profit rate for services was primarily driven by increased customer support costs due to share-based compensation and increased headcount and related costs in 2006 compared to 2005.

Operating Expenses. Operating expenses consist of selling and marketing, research and development, and general and administrative expenses, amortization of purchased intangible assets, and non-recurring litigation settlement costs. Total operating expenses increased 118% to $145.3 million for 2006, up from $66.8 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions. To a lesser extent, operating expenses increased as a result of inflationary increases in payroll and related costs, and increases in allocated corporate costs. As a percentage of revenue, total operating expenses were 82% for 2006 compared to 61% in 2005. This increase was primarily driven by the inclusion of costs not incurred in 2005, such as: share-based compensation of $9.6 million, amortization of purchased intangibles of $10.6 million, litigation settlement expense of $2.5 million, and one-time costs for severance due to acquisition related restructurings, duplicate and one-time integration costs, facility move costs and the write-off of an asset that was deemed to be fully impaired as a result of our acquisition of CipherTrust of $2.6 million. In addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates.

Selling and Marketing. Selling and marketing expenses consist primarily of salaries, commissions, share-based compensation and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, public relations, travel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Our customer support function, which provides support, training and installation services, is also responsible for supporting our sales representatives and sales engineers throughout the sales cycle by providing them and our prospective customers with technical assistance and, as such, a portion of those costs are included here. Selling and marketing expenses increased 100% to $84.5 million in 2006, up from $42.3 million in 2005. This increase was driven primarily by increased headcount and related costs along with severance for restructurings as a result of the CyberGuard and CipherTrust acquisitions, and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, the write-off of an asset that was deemed fully impaired as a result of the CipherTrust acquisition and inflationary increases in allocated corporate costs. As a percentage of revenue, selling and marketing expenses were 48% in 2006 compared to 39% in 2005. This increase was driven by one-time costs for our acquisitions, share-based compensation costs, and in addition, the acquired and assumed CyberGuard and CipherTrust expenses were higher as a percentage of revenue than our prior year stand-alone expense rates.

Research and Development. Research and development expenses consist primarily of salaries, share-based compensation and benefits for our product development and advanced technology personnel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Research and development expenses increased 103% to $34.1 million in 2006, up from $16.8 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, and inflationary increases in allocated corporate costs. As a percentage of revenue, research and development expenses were 19% for the year compared to 15% in 2005. This increase was driven by share-based compensation costs and in addition, the acquired and assumed CyberGuard and CipherTrust expense rates were higher as a percentage of revenue than our prior year stand-alone expenses.

Table of Contents

General and Administrative. General and administrative expenses consist primarily of salaries, share-based compensation, benefits and related expenses for our executive, finance and legal personnel, directors and officers insurance and allocations of corporate costs, which include information technology, facilities and human resources expenses. General and administrative expenses increased 89% to $13.6 million in 2006, up from $7.2 million in 2005. This increase was driven primarily by increased headcount and related costs as a result of the CyberGuard and CipherTrust acquisitions, legal fees, and to a lesser extent inflationary increases in payroll and related costs, share-based compensation costs, audit fees, and inflationary increases in allocated corporate costs. As a percentage of revenue, general and administrative expenses were 8% in 2006 compared to 7% in 2005. This increase was primarily due to duplicate costs incurred for the transitional employees due to the acquisitions.

Amortization of Purchased Intangible Assets. Amortization of purchased intangible assets consists of the amortization of tradenames and customer lists acquired in the CipherTrust and CyberGuard acquisitions, described in Note 2 and 3 of the Notes to the Consolidated Financial Statements, respectively, and to a lesser extent the N2H2 acquisition in 2003. Amortization of these acquired tradenames and customer lists was $10.6 million, or 6% of revenue, in 2006 compared to $496,000, or less than 1% of revenue, in 2005. This increase is due to the additional intangibles acquired in the CyberGuard and CipherTrust acquisitions.

Share-Based Compensation Expense. On January 1, 2006, we adopted Statement of Financial Accounting Standards (SFAS) No. 123(R), "Share-Based Payment," which requires the measurement and recognition of compensation expense for all share-based payment awards made to employees and directors including employee stock options and employee stock purchases based on estimated fair values. Share-based compensation expense related to stock options, restricted stock and shares purchased under our ESPP under SFAS 123(R) for the year ended December 31, 2006 was allocated as follows (in thousands):

	Year Ended December 31, 2006
Cost of product revenues	$ 357
Cost of service revenues	567
Selling and marketing	5,260
Research and development	2,542
General and administrative	1,830
Total share-based compensation expense	$ 10,556

There was no share-based compensation expense recognized for the year ended December 31, 2005.

Litigation Settlement. Litigation settlement expense of $2.5 million pertains to a charge related to litigation brought by the landlord of our former Concord, CA office. This expense represents a judgment in favor of the plaintiff for $1.1 million and additional costs of $1.4 million we incurred related to damages. The settlement was paid in July 2006.

Other (Expense)/Income. Other expense was $120,000 in 2006 as compared to other income of $1.6 million in 2005. The decrease is primarily a result of incurred interest expense related to debt assumed for the CipherTrust acquisition and a decrease in interest income on a decreased average cash balance.

Income Taxes. During 2006, we recorded income tax expense of $9.5 million. Of this $9.5 million income tax expense, a non-cash expense of $8.5 million is related to a net tax valuation allowance recorded on our net deferred tax assets. We were unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses, and needed to provide tax expense for the subsequent valuation allowance reapplied to the remaining net operating losses. This was a result of changes in circumstances due to recent acquisitions that caused a change in judgment regarding the realizability of our net deferred tax assets in the fourth quarter. The remainder of the income tax expense is related to current income tax components such as, alternative minimum income tax, and state and foreign income taxes. This is compared with $608,000 of income tax expense recorded in 2005 which consisted of $349,000 for alternative minimum tax expense, $58,000 for state income tax expense and $201,000 for various foreign income tax expenses.

Table of Contents

Federal alternative minimum tax was provided on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carryforward which we have available. Similar to 2006, we anticipate that we will be in an alternative minimum taxable income position in 2007. Current tax law provides that part or all of the amount of the alternative minimum tax paid can be carried forward indefinitely and credited against federal regular tax in future tax years to the extent the regular tax liability exceeds the alternative minimum tax in those years. For 2006, the reversal of $3.1 million of the tax valuation allowance related to acquired net operating losses was recorded as a decrease to goodwill in the balance sheet and not as a benefit to tax expense in the income statement.

In accordance with SFAS No. 109, we have assessed the likelihood that the net deferred tax assets will be realized. SFAS No. 109, "Accounting for Income Taxes," requires the consideration of a valuation allowance in all circumstances, if the conclusion is not more likely than not a valuation allowance is required. We have determined that it is more likely than not that deferred tax assets of $24.4 million at December 31, 2006 will be realized based on our expected future reversals of certain deferred tax liabilities. We have a net deferred tax liability recorded in our balance sheet that consists primarily of indefinite lived intangible assets that are not deductible for tax purposes and therefore cannot be used to realize additional reversing deferred tax assets. In accordance with SFAS No. 109, our remaining noncurrent deferred tax liabilities are netted with our noncurrent deferred tax assets and are presented as a single amount in our consolidated balance sheet.

Worldwide net operating loss carryforwards totaled approximately $479.5 million at December 31, 2006, comprised of $456.6 million domestic net operating loss carryforwards and $22.9 million of international net operating loss carryforwards. These carryforwards are available to offset taxable income through 2026 and will start to expire in 2011. Of these carryforwards, $208.1 million relates to acquired CyberGuard net operating losses, $59.6 million relates to acquired N2H2 net operating losses, and $19.4 million relates to acquired CipherTrust net operating losses. We have provided a complete valuation allowance on primarily all of these acquired losses are fully valued against, and upon release of the valuation allowance, a portion of the benefit will go to the balance sheet to reduce goodwill instead of a benefit to the income tax provision. As of December 31, 2006 we have deducted $56.8 million related to stock option exercises. The tax benefit in excess of book expense from these stock option exercises will be recorded as an increase to additional paid-in capital upon utilization of the net operating losses under the financial statement approach to recognizing the tax benefits associated with stock option deductions. Of the remaining benefit associated with the carryforwards, approximately $111.3 million has yet to be recognized in the consolidated statement of operations. However, there are no assurances that the tax benefit of these carryforwards will be available to offset future income tax expense when taxable income is realized.

As a matter of course, we are regularly audited by federal, state, and foreign tax authorities. From time to time, these audits result in proposed assessments. During the fourth quarter of 2006, we reached a settlement with the Internal Revenue Service regarding all assessments proposed with respect to the CipherTrust federal income tax return for 2004. The Internal Revenue Service has commenced its examination of CipherTrusts federal income tax returns for 2003 and 2005. In our opinion, the final resolution of these audits will not have a material adverse effect on our consolidated financial position, liquidity or results of operations. We anticipate the completion of these field audits during 2007.

Estimates were used in the determination of our provision for income taxes, current income taxes payable, as well as in our deferred tax asset and liability analysis. These estimates take into account current tax laws and our interpretation of these current tax laws within the various taxing jurisdictions within which we operate. Changes in the tax laws or our interpretation of tax laws and the resolution of future audits could impact our provision for income taxes.

Comparison of Years Ended December 31, 2005 and 2004.

Revenues. Our total revenues increased 17% to $109.2 million in 2005, up from $93.4 million in 2004. Our product revenues increased 17% to $79.3 million in 2005, up from $67.6 million in 2004. Our service

Table of Contents

revenues increased 16% to $29.8 million in 2005, up from $25.8 million in 2004. The increase in total revenues in 2005 was driven by growth across all product lines. Our Network Gateway Security revenue (formerly known as the Sidewinder G2 Firewall product line) increase was due to increased demand for our security appliance. Our Web Gateway Security revenue (formerly known as the Web filtering product line) increase was due to continued traction through OEM relationships. The Identity and Access Management revenue (formerly known as the SafeWord product line) increase was driven by sustained demand for high assurance solutions.

Cost of Revenues and Gross Profit. Total cost of revenues, which includes products and services costs, increased 27% to $22.0 million in 2005, up from $17.4 million in 2004. This increase is the direct result of the increase in total revenues. Gross profit as a percentage of revenue decreased from 81% in 2004 to 80% in 2005. Gross profit for products decreased to 79% in 2005 compared to 82% in 2004. This decline was driven by increased sales volume on products containing a hardware component, primarily the SafeWord token sales, which have a lower gross profit margin than our software products. Gross margins were also reduced as a result of a larger portion of business being transacted with channel partners versus direct to end users in 2005 as compared to 2004. Gross profit for services was 83% in 2005 compared to 80% in 2004. The improvement in the gross profit rate for services was primarily driven by our services revenue growth outpacing the growth of our services costs in 2005 compared to 2004.

Operating Expenses. Operating expenses consist of selling and marketing, research and development, and general and administrative expenses. Total operating expenses increased 5% to $66.8 million for 2005, up from $63.8 million in 2004. This increase was driven primarily by an inflationary increase in payroll and related costs and inflationary increases in corporate costs. As a percentage of revenue, total operating expenses were 61% for 2005 compared to 68% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of operating expenses during 2005 compared to 2004.

Selling and Marketing. Selling and marketing expenses consist primarily of salaries, commissions, and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, public relations, travel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Selling and marketing expenses increased 3% to $42.3 million in 2005, up from $41.2 million in 2004. This increase was driven primarily by inflationary increases in payroll and related costs, an increase in commission expense due to expanding revenues, and inflationary increases in allocated corporate costs. As a percentage of revenue, selling and marketing expenses were 39% in 2005 compared to 44% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of selling and marketing expenses during 2005 compared to 2004.

Research and Development. Research and development expenses consist primarily of salaries and benefits for our product development personnel and allocations of corporate costs, which include information technology, facilities and human resources expenses. Research and development expenses increased 5% to $16.8 million in 2005, up from $16.1 million in 2004. This increase was driven by inflationary increases in payroll, benefits and allocated corporate costs. As a percentage of revenue, research and development expenses were 15% for the year compared to 17% in 2004. This improvement was primarily driven by revenue growth outpacing the growth of research and development expenses during 2005 compared to 2004.

General and Administrative. General and administrative expenses consist primarily of salaries, benefits and related expenses for our executive, finance and legal personnel, directors and officers insurance and allocations of corporate costs, which include information technology, facilities and human resources expenses. General and administrative expenses increased 11% to $7.2 million in 2005, up from $6.5 million in 2004. This increase was driven primarily by an increase in audit and legal fees, inflationary increases in allocated corporate costs, and to a lesser extent, inflationary increases in payroll and benefits. As a percentage of revenue, general and administrative expenses were 7% in both 2005 and 2004. This rate remained consistent compared to prior year, despite the increase in our general and administrative expenses, due to revenue growth being consistent with the growth of general and administrative expenses in 2005 compared to 2004.

Table of Contents

Other Income. Other income was $1.6 million in 2005, an increase from $607,000 in 2004. The increase reflects higher interest rates on higher cash balances in 2005 as compared to 2004.

Income Taxes. We incurred tax expenses of $608,000, consisting of $349,000 for U.S. Federal alternative minimum tax expense, $58,000 for state income tax expense, and $201,000 for various foreign income taxes, in 2005 compared to no tax expense recognized in 2004. Federal alternative minimum tax was provided for in 2005 on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carry forward which we have available. This is in accordance with applicable tax law. The tax position provided for in the income tax provisions prior to 2005 did not include alternative minimum taxable income. Tax expense of $283,000 incurred for various foreign income taxes and $62,000 incurred for state income tax in 2004 was offset by the reversal of a like amount of the previously established valuation allowance against our deferred tax asset. We have assessed the likelihood that our net deferred tax assets will be realized. The computations of our deferred tax assets and valuation allowance are based on taxable income we expect to earn on sales of existing products, and projected interest and other income over the next three years. Realization of the $3.6 million of net deferred tax assets is dependent upon our ability to generate sufficient future taxable income and the implementation of tax planning strategies. We have determined that it is more likely than not that the net deferred tax assets will be realized based on expected levels of future taxable income in the U.S. and certain foreign jurisdictions and the implementation of tax planning strategies. Our expectations regarding future profitability may change due to future market conditions, changes in tax laws and other factors. Future taxable income of $9.4 million is required to realize the $3.6 million deferred tax asset at December 31, 2005. We had total net operating loss carryforwards of approximately $177.7 million at December 31, 2005. Of these carryforwards, $49.9 million relates to stock option exercises and $59.6 million relates to acquired N2H2 net operating losses, which currently have a full valuation allowance, and when realized for financial statement purposes will not result in a reduction in income tax expense. Rather, the benefit from the stock option exercises will be recorded as an increase to additional paid-in capital and the benefit from the N2H2 net operating loss carryforwards will be recorded as a decrease to goodwill. Of the remaining benefit associated with the carryforwards, approximately $58.8 million have yet to be recognized as a benefit in the consolidated statement of operations. However, there are no assurances that these carryforwards will be available to offset future income tax expense when taxable income is realized.

Deferred taxes are required to be measured at the regular tax rate. An analysis recently completed of our regular tax rate, indicated that our tax rate had changed. Accordingly the deferred tax components, including the valuation allowance, were adjusted as a result of applying the appropriate rate. The deferred tax components include the benefit of the alternative tax credit carry forward. See Note 12 of the Notes to the Consolidated Financial Statements regarding the tax effect of these items in 2005.

Estimates were used in the determination of our provision for income taxes, current income taxes payable, as well as in our deferred tax asset and liability analysis. These estimates take into account current tax laws and our interpretation of these current tax laws within the various taxing jurisdictions within which we operate. Changes in the tax laws or our interpretation of tax laws and the resolution of future audits could impact our provision for income taxes.

Liquidity and Capital Resources

At December 31, 2006, our principal source of liquidity was $8.2 million of cash, representing a $41.8 million decrease from December 31, 2005. Our investments decreased $30.7 million from $31.1 million at December 31, 2005 to $457,000 at December 31, 2006. These decreases were primarily due to $95.0 million in cash paid directly by us to CipherTrust shareholders for the CipherTrust acquisition, $18.9 million in cash paid directly by us to CyberGuard shareholders for the CyberGuard acquisition, offset by $36.1 million provided by operating activities and $8.1 million from the exercise of stock options and sale of common stock through our employee stock purchase plan (ESPP). At December 31, 2006, we have future payments of $138.5 million on our debt commitment and net future payments under non-cancelable operating leases of $23.2 million. We expect to generate cash during 2007 as we expect billings to continue to grow at a faster rate than operating expenses.

Table of Contents

Last year we financed our operations primarily with cash generated from operations, as well as through sales of our equity securities and borrowings on our credit facility. In 2006, we utilized and paid back $8.5 million on our $20.0 million revolving credit facility.

Net cash provided by operating activities of $36.1 million for the twelve months ended December 31, 2006, was comprised of $41.8 million in net non-cash related expenses, a $43.9 million increase in deferred revenue, and a $8.4 million increase in accounts payable and accrued payroll offset by a $27.4 million net loss, a $12.1 million increase in accounts receivable, a $4.3 million decrease in accrued expenses and a $14.3 million decrease in acquisition reserves. Net cash provided by operations was driven by the increase in our billings outpacing the increase in our operating expenses. Terms for cash collections received from customers and cash payments made to vendors were consistent with normal business practices.

Net cash used in investing activities of $239.3 million for the twelve months ended December 31, 2006, consisted of a $187.7 million cash outlay for the acquisition of CipherTrust, $69.1 million cash outlay for the acquisition of CyberGuard, and $11.8 million for capital additions, net of $31.0 million in cash received from net sales/maturities of investments. The capital additions were used for furnishing our new St. Paul, Minnesota facility, computer equipment and technology upgrades.

Net cash provided by financing activities of $163.0 million for the twelve months ended December 31, 2006 consisted primarily of $84.9 million received from debt financing, net of transaction fees of $3.1 million and a principal repayment of $2.0 million, which was used to finance the CipherTrust acquisition, $69.9 million received from the issuance of preferred stock, net of transaction fees, which was used to finance the CyberGuard acquisition, and $8.1 million related to the exercise of stock options and sale of common stock through our ESPP.

We anticipate using available cash to fund growth in operations, invest in capital equipment, acquire businesses, license technology or products related to our line of business, and make additional payments on our long-term debt. We expect to spend approximately $12.0 million on capital expenditures in 2007.

A summary of our total contractual cash obligations as of December 31, 2006 is as follows (in thousands):

		Payments Due by Period			
	Total	Less Than One Year	One to Three Years	Three to Five Years	After Five Years
Operating leases, net of subleases	$ 23,233	$ 5,264	$ 7,419	$ 4,196	$ 6,354
Principal and interest payments on debt	$138,509	$ 7,730	$ 16,290	$ 16,877	$ 97,612
Total contractual cash obligations	$161,742	$12,994	$ 23,709	$ 21,073	$103,966

We believe that we have sufficient financial resources available to fund our current working capital and capital expenditure requirements for at least the next twelve months. In addition to the cash on hand, we have a $20.0 million revolving credit facility available pursuant to a credit facility agreement with a syndicate of banks led by Citigroup and UBS Investment Bank which was signed in August 2006. We intend to utilize the funds available through the credit facility for general working capital and ongoing corporate purposes as deemed necessary.

Our credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain financial covenants, on a quarterly basis, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We are in compliance with all covenants as of December 31, 2006.

Disclosures about Off-Balance Sheet Arrangements

We did not have any off-balance sheet arrangements as of December 31, 2006 or 2005.

Table of Contents

Critical Accounting Policies and Estimates

Our discussion of the financial condition and results of operations are based upon the consolidated financial statements, which have been prepared in conformity with U.S. generally accepted accounting principles. The preparation of our financial statements requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, revenues and expenses, and related disclosure of any contingent assets and liabilities at the date of the financial statements. Management regularly reviews its estimates and assumptions, which are based on historical factors and other factors that are believed to be relevant under the circumstances. Actual results may differ from these estimates under different assumptions, estimates, or conditions.

Critical accounting policies are defined as those that are reflective of significant judgments and uncertainties, and potentially result in materially different results under different assumptions and conditions. See Note 1 of the Notes to Consolidated Financial Statements for additional discussion of the application of these and other accounting policies.

Revenue Recognition. We derive our revenue primarily from two sources: (i) sales of products, including hardware, subscriptions, software licenses, and royalties and (ii) sales of services, including maintenance arrangements to provide upgrades and customer support, professional services, and contracted development work. We recognize revenue in accordance with Statement of Position (SOP) 97-2, "Software Revenue Recognition," as modified by SOP 98-9. Revenue from products is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed and determinable, and collection is probable. Subscription-based contracts are generally for 12, 24 or 36 months in duration. Subscription revenue along with maintenance revenue for providing product upgrades and customer support are deferred and recognized ratably over the service period beginning with the month the subscription or service begins.

When arrangements contain multiple elements and vendor specific objective evidence (VSOE) of fair value exists for all undelivered elements, we recognize revenue for the delivered elements using the residual method. For arrangements containing multiple elements where VSOE of fair value does not exist for all undelivered elements, we defer revenue for the delivered and undelivered elements and then recognize revenue on all elements over the service period. In instances where an entire arrangement is deferred due to lack of VSOE of fair value on an undelivered element, the revenue recognized over the service period is allocated to products and services revenue based on the value of the elements as presented on the customer's purchase order which approximates an allocation proportionate to our list price. We also identify costs (primarily hardware component costs) that are directly associated with product revenues that have been deferred due to lack of VSOE of fair value on an undelivered element and we defer these costs at the time of shipment and recognize them as cost of sales in proportion to the product revenue as it is recognized over the service term.

We sell our products either directly to an end-user, or indirectly through our channel of resellers and distributors (our channel partners). When selling through our channel we require our channel partners to provide evidence of end-user sell-through. If we are unable to obtain end-user evidence at the time we fulfill the order from a channel partner, we do not recognize revenue until the channel partner supplies end-user information, the product has been shipped, and all other criteria of SOP 97-2 have been met, with the exception of sales to our distributors who stock our SnapGear product line. We recognize revenue, net of estimated returns, upon shipment of our SnapGear product line as we have sufficient return history to establish a reserve and we are not able to receive end-user evidence due to the high-volume sales of this low-price point product.

Allowance for Doubtful Accounts. We make estimates regarding the collectibility of our accounts receivables. When we evaluate the adequacy of our allowance for doubtful accounts, we consider multiple factors including historical write-off experience, the need for specific customer reserves, the aging of our receivables, customer creditworthiness, changes in our customer payment cycles, and current economic trends. Historically, our allowance for doubtful accounts has been adequate based on actual results. If the financial condition of our customers were to deteriorate, resulting in an impairment of their ability to make payments, additional allowances may be required.

Business Combinations. When we acquire businesses, we allocate the purchase price to tangible assets and liabilities and identifiable intangible assets acquired. Any residual purchase price is recorded as goodwill. The allocation of the purchase price requires management to make significant estimates in determining the fair values of assets acquired and liabilities assumed, especially with respect to intangible assets. These estimates are based on historical experience and information obtained from the management of the acquired companies. These estimates can include, but are not limited to, the cash flows that an asset is expected to generate in the future, the appropriate weighted average cost of capital, and the cost savings expected to be derived from acquiring an asset. These estimates are inherently uncertain and unpredictable. In addition, unanticipated events and circumstances may occur which may affect the accuracy or validity of such estimates.

We assess the impairment of goodwill annually, or more often if events or changes in circumstances indicate that the carrying value may not be recoverable. We evaluate goodwill for impairment by comparing the fair value of our reporting unit to its carrying value, including the goodwill allocated to that reporting unit. To determine our reporting unit's fair value in the current year evaluation, we used a valuation technique based on multiples of revenue. If management's estimates of future operating results change, or if there are changes to other assumptions, the estimate of the fair value of our goodwill could change significantly. Such change could result in goodwill impairment charges in future periods, which could have a significant impact on our consolidated financial statements.

We assess the impairment of acquired developed technology and other identifiable intangible assets whenever events or changes in circumstances indicate that an asset's carrying amount may not be recoverable. An impairment loss would be recognized when the sum of the estimated future cash flows expected to result from the use of the asset and its eventual disposition is less than its carrying amount. Such impairment loss would be measured as the difference between the carrying amount of the asset and its fair value. Our cash flow assumptions are based on historical and forecasted revenue, operating costs, and other relevant factors. If management's estimates of future operating results change, or if there are changes to other assumptions, the estimate of the fair value of our acquired developed technology and other identifiable intangible assets could change significantly. Such change could result in impairment charges in future periods, which could have a significant impact on our consolidated financial statements.

Deferred Tax Assets. We account for income taxes under SFAS No. 109, "Accounting for Income Taxes," which requires recognition of deferred tax liabilities and assets for the expected future tax consequences of events that have been included in our financial statements or tax returns. Under this method, deferred tax liabilities and assets are determined based on the difference between the financial statement and tax basis of assets and liabilities, using enacted tax rates in effect for the year in which the differences are expected to reverse. SFAS No. 109 requires the consideration of a valuation allowance for deferred tax assets if it is "more likely than not" that some component or all of the benefits of deferred tax assets will not be realized.

Share-Based Compensation. Prior to January 1, 2006, we accounted for share-based employee compensation plans under the measurement and recognition provisions of Accounting Principles Board (APB) Opinion No. 25, "Accounting for Stock Issued to Employees," and related Interpretations, as permitted by SFAS No. 123, "Accounting for Stock-Based Compensation." Accordingly, we recorded no share-based employee compensation expense for options granted under our current stock option plans during the year ended December 31, 2005 as all options granted under those plans had exercise prices equal to the fair market value of our common stock on the date of grant. We also recorded no compensation expense in those periods in connection with our Employee Stock Purchase Plan (ESPP) as the purchase price of the stock was not less than 85% of the lower of the fair market value of our common stock at the beginning of each offering period or at the end of each purchase period. In accordance with SFAS No. 123 and SFAS No. 148, "Accounting for Stock-Based Compensation – Transition and Disclosure," we provided pro forma net income and net income per share disclosures for each period prior to the adoption of SFAS No. 123(R), "Share-Based Payment," as if we had applied the fair value-based method in measuring compensation expense for our share-based compensation plans.

Table of Contents

Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R), using the modified prospective transition method. Under that transition method, we recognized compensation expense for share-based payments that vested during the year ended December 31, 2006 using the following valuation methods: (a) for share-based payments granted prior to, but not yet vested as of, January 1, 2006, the grant date fair value was estimated in accordance with the original provisions of SFAS No. 123, and (b) for share-based payments granted on or after January 1, 2006, the grant date fair value was estimated in accordance with the provisions of SFAS No. 123(R). Because we elected to use the modified prospective transition method, results for prior periods have not been restated. In March 2005, the Securities and Exchange Commission issued Staff Accounting Bulletin (SAB) No. 107, "Share-Based Payment," which provides supplemental implementation guidance for SFAS No. 123(R). We have applied the provisions of SAB No. 107 in our adoption of SFAS No. 123(R). We estimate the fair value of stock options granted and the discount offered through our ESPP using the Black Scholes model, which requires the input of highly subjective assumptions. See Note 10 for information on the impact of our adoption of SFAS No. 123(R) and the assumptions we use to calculate the fair value of share-based employee compensation. In addition, we began offering restricted shares in 2006 and we intend to continue to do so in the future.

Derivative Instrument. In September 2006, we entered into an interest rate cap agreement which is required to be accounted for under SFAS No. 133, "Accounting for Derivative Instruments and Hedging Activities." SFAS No. 133 establishes accounting and reporting standards for derivative instruments, including certain derivative instruments embedded in other contracts, and for hedging activities. It requires that an entity recognize all derivatives as either assets or liabilities in the statement of financial position and measure those instruments at fair value. If certain conditions are met, a derivative may be specifically designated as (a) a hedge of the exposure to changes in the fair value of a recognized asset or liability or an unrecognized firm commitment, (b) a hedge of the exposure to variable cash flows of a forecasted transaction, or (c) a hedge of the foreign currency exposure of a net investment in a foreign operation, an unrecognized firm commitment, an available-for-sale security, or a foreign-currency-denominated forecasted transaction. Our interest rate cap agreement applies to (b), referred to as a cash flow hedge. For a derivative that is designated as a cash flow hedge the effective portion of the derivative's gain or loss is initially reported as a component of other comprehensive income and subsequently reclassified into earnings when the forecasted transaction affects earnings. The ineffective portion of the gain or loss is immediately recognized in income.

Inflation

To date, we have not been significantly affected by inflation.

Recently Issued Accounting Standards

In July 2006, the FASB issued Interpretation No. 48 (FIN 48), "Accounting for Uncertainty in Income Taxes, an Interpretation of SFAS No. 109." FIN 48 creates a single model to address accounting for uncertainty in tax positions and clarifies the accounting for income taxes by prescribing the minimum recognition threshold a tax position is required to meet before being recognized in the financial statements. Specifically under FIN 48, the tax benefits from an uncertain tax position may be recognized only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities, based upon the technical merits of the position. FIN 48 also provides guidance on de-recognition, measurement, classification, interest and penalties, accounting in interim periods, disclosure and transition. FIN 48 is effective for fiscal years beginning after December 15, 2006. As prescribed in the interpretation, the cumulative effect of applying the provisions of FIN 48 will be reported as an adjustment to the opening balance of retained earnings at January 1, 2007. We will adopt FIN 48 effective January 1, 2007 as required. We are currently evaluating the potential impact which the adoption of FIN 48 will have on our financial position, cash flows, and results of operations.

In September 2006, the FASB issued SFAS No. 157, "Fair Value Measurements." SFAS No. 157 establishes a framework for measuring fair value in generally accepted accounting principles, clarifies the

EXHIBIT 26
PART 2

definition of fair value within that framework, and expands disclosures about the use of fair value measurements. SFAS No. 157 is intended to increase consistency and comparability among fair value estimates used in financial reporting. As such, SFAS No. 157 applies to all other accounting pronouncements that require (or permit) fair value measurements, except for the measurement of share-based payments. SFAS No. 157 does not apply to accounting standards that require (or permit) measurements that are similar to, but not intended to represent, fair value. Fair value, as defined in SFAS No. 157, is the price to sell an asset or transfer a liability and therefore represents an exit price, not an entry price. The exit price is the price in the principal market in which the reporting entity would transact. Further, that price is not adjusted for transaction costs. SFAS No. 157 is effective for fiscal years beginning after November 15, 2007, and interim periods within those fiscal years. SFAS No. 157 will be applied prospectively as of the beginning of the fiscal year in which it is initially applied. We are currently assessing the impact of adoption of SFAS No. 157.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We develop products in the U.S., Australia, and Germany and sell them worldwide. As a result, our financial results could be affected by factors such as changes in foreign currency exchange rates or weak economic conditions in foreign markets. Since our sales are currently priced in U.S. dollars, a strengthening of the dollar could make our products less competitive in foreign markets and our accounts receivable more difficult to collect.

We believe that our international entities are subject to risks typical of any international entity, including, but not limited to: differing economic conditions, changes in political climate, differing tax structures, other regulations and restrictions, and foreign exchange rate volatility. Accordingly, our future results could be materially adversely impacted by changes in these or other factors.

We are exposed to market risk from changes in the interest rates on certain outstanding debt. As of December 31, 2006, we had $88.0 million of outstanding indebtedness. Of this indebtedness, approximately $28.0 million bears interest at rates that fluctuate with changes in certain prevailing interest rates. Based on the average outstanding debt for fiscal 2006, a 100 basis point change in interest rates would change interest expense by approximately $300,000 in fiscal 2007.

We also hold an equity interest in a privately held technology company. This investment was recorded at cost and is reported in other assets on our consolidated balance sheets. As of December 31, 2006 this investment had a carrying value of $2.7 million.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

Our financial statements required by this item are set forth as a separate section of this report. See Part IV, Item 15 of this Form 10-K.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURE

Not applicable.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

Management of our company is responsible for establishing and maintaining effective disclosure controls and procedures, as defined under Rules 13a-15(e) and 15d-15(e) of the Securities Exchange Act of 1934. At December 31, 2006, an evaluation was performed, under the supervision and with the participation of management, including our Chief Executive Officer and Chief Financial Officer, of the effectiveness of the design and operation of our disclosure controls and procedures. Based upon that evaluation, the Chief Executive

Officer and Chief Financial Officer concluded that as of December 31, 2006, our disclosure controls and procedures were not effective at the reasonable assurance level, as a result of a material weakness in the internal controls related to accounting for income taxes, to ensure that information required to be disclosed in the Annual Report on Form 10-K was recorded, processed, summarized and reported within the time period required by the Securities and Exchange Commission's rules and forms and accumulated and communicated to management, including our Chief Executive Officer and Chief Financial Officer, to allow timely decisions regarding required disclosure.

Changes in Internal Control Over Financial Reporting

During the quarter ended December 31, 2006, there have been no changes in our internal control over financial reporting that materially affected, or are reasonably likely to materially affect, our internal control over financial reporting, except those relating to the acquisition of CipherTrust, Inc. as of December 31, 2006 and the material weakness indentified below. See Note 2 of the Notes to the Consolidated Financial Statements included in Item 15 for discussion of the acquisition and related financial data. We are in the process of integrating the CipherTrust operations and will be incorporating these operations as part of our internal controls. However, for purposes of this evaluation, the impact of this acquisition on our internal controls over financial reporting has been excluded.

Management's Report on Internal Control Over Financial Reporting

Our management is responsible for establishing and maintaining adequate internal control over financial reporting as defined in Rules 13a-15(f) under the Securities Exchange Act of 1934. Our internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with accounting principles generally accepted in the United States. Internal control over financial reporting includes those written policies and procedures that:

- pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of our assets;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with accounting principles generally accepted in the United States of America;
- provide reasonable assurance that our receipts and expenditures are being made only in accordance with authorization of our management and directors; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of assets that could have a material effect on the consolidated financial statements.

Internal control over financial reporting includes the controls themselves, monitoring and internal auditing practices and actions taken to correct deficiencies as identified.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

A material weakness in internal control over financial reporting is a significant deficiency (within the meaning of PCAOB Auditing Standard No. 2), or combination of significant deficiencies, that results in there being more than remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected by employees in the normal course of performing their assigned functions.

Management assessed the effectiveness of our internal control over financial reporting as of December 31, 2006. In making this assessment, management used the criteria set forth by the Committee of Sponsoring

Organizations of the Treadway Commission (COSO) in Internal Control – Integrated Framework. Management's assessment included an evaluation of the design of our internal control over financial reporting and testing of the operational effectiveness of its internal control over financial reporting. Management reviewed the results of its assessment with the Audit Committee of our Board of Directors.

Based on this assessment, management identified, as of December 31, 2006, a material weakness existed in the company's internal control over financial reporting related to the accounting for income taxes. There were ineffective controls relating to the review of our year-end tax provision, including review of the tax technical accounting items where our outside tax consultants typically provide input. This control deficiency resulted in a material misstatement of various income tax balances that was not prevented or detected by management. As a result, material errors in accounting for income taxes occurred, which were corrected prior to the issuance of the annual financial statements. Accordingly management has determined this control deficiency constitutes a material weakness.

Due to the material weakness described above, management concluded that, as of December 31, 2006, the Company's system of internal control over financial reporting related to accounting for income taxes was not effective based on the criteria established in Internal Control—Integrated Framework.

Management's assessment of the effectiveness of internal control over financial reporting as of December 31, 2006 excluded the business operations of CipherTrust, Inc., acquired on August 31, 2006. The acquired business operations excluded represent $66.0 million and $19.1 million of total and net assets, respectively, and $7.1 million of revenues of our related consolidated financial statement amounts as of and for the year ended December 31, 2006.

Our management's assessment of the effectiveness of our internal control over financial reporting as of December 31, 2006 has been audited by Ernst & Young LLP, an independent registered public accounting firm, as stated in their report which is included herein on page 78.

Remediation Plan for Material Weakness in Accounting for Income Taxes

In 2006 we experienced an increased level of complexity in our accounting for income taxes as the result of the CyberGuard and CipherTrust acquisitions which occurred during the year. As a result of this increased complexity we have engaged our outside tax consultants to assist in the review of our tax provision in order for us to have effective review controls over our accounting for income taxes. The review of our tax provision workpapers for the period ended December 31, 2006 was ineffective and the review by our outside tax consultants did not occur, resulting in a material weakness. To remediate the identified material weakness, management plans to ensure that the appropriate levels of review by management and involvement of outside tax consultants will take place in a timely manner in future periods.

Table of Contents

PART III

ITEM 10. DIRECTORS AND EXECUTIVE OFFICERS OF THE REGISTRANT

Incorporated herein by reference is the information under the heading "Election of Directors," "Section 16(a) Beneficial Ownership Reporting Compliance," and "Committees of the Board of Directors," in our Proxy Statement to be filed on or about March 30, 2007. See also Part I, Item 1, "Executive Officers" of this Form 10-K.

We maintain a Code of Business Conduct and Ethics applicable to all our employees. We have also adopted a Code of Ethics for Finance that is applicable to our Chief Executive Officer, Chief Financial Officer, Vice President of Finance, and finance personnel performing functions related to financial reporting. A copy of our Code of Business Conduct and Ethics and our Code of Ethics for Finance, as well as our corporate governance guidelines and the committee charters for each of the committees of the Board of Directors, can be obtained from our Internet website at **www.securecomputing.com** under the Investor Relations page and will be made available free of charge to any shareholder upon request. We intend to disclose any waivers from, or amendments to, the Code of Business Conduct and Ethics and Code of Ethics for Finance by posting a description of such waiver or amendment on our Internet website. However, we have never granted a waiver from either the Code of Business Conduct and Ethics and Code of Ethics for Finance.

ITEM 11. EXECUTIVE COMPENSATION

Incorporated herein by reference is the information appearing in our Proxy Statement which we anticipate filing on or about March 30, 2007, under the headings "Election of Directors," "Compensation Discussion and Analysis (CD&A)," "Compensation Committee Report," "Summary Compensation Table," "2006 Grants of Plan-Based Awards," "2006 Outstanding Equity Awards at Fiscal Year-End," "2006 Option Exercises and Stock Vested," "Director Compensation," and "2006 Potential Payments Upon Termination or Change in Control."

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT

Incorporated herein by reference is the information appearing under the heading "Security Ownership of Principal Stockholders and Management" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

Equity Compensation Plan Information

The following table sets forth information regarding securities authorized for issuance under equity compensation plans:

Plan category	Number of securities to be issued upon exercise of outstanding options, warrants and rights	Weighted-average exercise price of outstanding options, warrants and rights	Number of securities remaining available for future issuance under equity compensation plans
Equity compensation plans approved by stockholders (1)(2)(3)(4)(5)	13,182,418	$ 9.92	2,367,523
Equity compensation plans not approved by stockholders (6)	3,678,134	4.97	510,197
Total	16,860,552	$ 8.84	2,877,720

(1) In September 1995, our Board of Directors and stockholders approved our 1995 Omnibus Stock Plan. Under the terms of this Plan, key employees and non-employees may be granted options to purchase up to 11,494,131 shares of our Common Stock. The majority of options granted under this plan have ten year terms and vest either annually over three years, or fully vest at the end of three years. Beginning in 2003, all new stock options granted under this plan vest 25% after the first year and then monthly over the following three years. This plan expired in September 2005.

Table of Contents

(2) In connection with our acquisition of N2H2, Inc. in October 2003, we assumed all of the outstanding N2H2 stock options under the 1997 Stock Option Plan, 1999 Stock Option Plan, 1999 Non-Employee Director Plan, 1999/2000 Transition Plan, the 2000 Stock Option Plan, and the Howard Philip Welt Plan (the "N2H2 Plans"), which were converted into options to purchase approximately 420,000 shares of our common stock. All stock options assumed were exercisable and vested. These options were assumed at prices between $1.55 and $258.63 per share, with a weighted average exercise price of $9.45 per share. The options granted under these plans have ten year terms and vest 25% after the first year and then monthly over the following three years.

(3) In connection with our acquisition of CyberGuard in January 2006, we assumed all of the outstanding CyberGuard stock options under the 1994 and 1998 Stock Option Plans which were converted into options to purchase 3,039,545 shares of our common stock. All outstanding stock options assumed were exercisable and vested. These options were assumed at prices between $1.56 and $15.07 per share, with a weighted average exercise price of $7.21 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

(4) In July 2002, our Board of Directors and Compensation Committee approved our 2002 Stock Incentive Plan. In September 2005, our Board of Directors and Compensation Committee approved an amendment and restatement of our 2002 Stock Incentive Plan. Our stockholders approved the amendment and restatement on January 11, 2006. Under the terms of this Plan, key employees and non-employees may be granted options, restricted stock awards, restricted stock units, stock appreciation rights and other similar types of stock awards to purchase up to 6,500,000 shares of our Common Stock. The options granted in 2002 have ten year terms and vest either annually over three years, or fully vest at the end of three years. Beginning in 2003, all options granted under this plan vest 25% after the first year and then monthly over the following three years for employees. Restricted stock awards vest 25% after the first year, then quarterly thereafter over the following three years, unless otherwise approved by the Compensation Committee. All awards granted to non-employee directors vest 100% after the first year.

(5) In connection with our acquisition of CyberGuard in January 2006, we issued a warrant to purchase 1,000,000 shares of our Common Stock pursuant to a securities purchase agreement with Warburg Pincus. The warrant is exercisable at $13.85 per share.

(6) In connection with our acquisition of CipherTrust in August 2006, we assumed all of the outstanding CipherTrust stock options under the 2000 Stock Option Plan which were converted into options to purchase 2,543,662 shares of our common stock. All outstanding stock options assumed were unvested and have seven-year terms. These options were assumed at prices between $0.01 and $6.19 per share, with a weighted average exercise price of $2.88 per share. After the date of acquisition, the options granted under these plans have ten year terms and vest 25% after the first year and then monthly over the following three years.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS

Incorporated herein by reference is the information appearing under the heading "Certain Transactions" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

Incorporated herein by reference is the information appearing under the heading "Relationship with Independent Registered Public Accounting Firm" in our Proxy Statement that we anticipate filing on or about March 30, 2007.

Table of Contents

PART IV

ITEM 15. EXHIBITS, FINANCIAL STATEMENT SCHEDULES, AND REPORTS ON FORM 8-K

(a) The following documents are filed as part of this report:

1. Consolidated Financial Statements:

   Consolidated Balance Sheets as of December 31, 2006 and 2005
   Consolidated Statements of Operations for the years ended December 31, 2006, 2005 and 2004
   Consolidated Statements of Stockholders' Equity for the years ended December 31, 2006, 2005 and 2004
   Consolidated Statements of Cash Flows for the years ended December 31, 2006, 2005 and 2004
   Notes to Consolidated Financial Statements
   Report of Independent Registered Public Accounting Firm
   Report of Independent Registered Public Accounting Firm – Section 404

2. Consolidated Financial Statement Schedule:

   Schedule II – Valuation and Qualifying Accounts. Such schedule should be read in conjunction with the consolidated financial statements. All other supplemental schedules are omitted because of the absence of conditions under which they are required.

(b) Reports on Form 8-K:

On November 14, 2006, we filed an Amendment No. 1 on Form 8-K/A which amends and supplements the Current Report on Form 8-K filed by us on September 7, 2006 pursuant to Item 2.01, "Completion of Acquisition or Disposition of Assets," announcing that on August 31, 2006, we completed the purchase of substantially all of the assets of CipherTrust, Inc. This Amendment No. 1 was filed to include the financial information pursuant to Item 9.01, "Financial Statements and Exhibits."

(c) Exhibits required to be filed by Item 601 of Regulation S-K:

The following exhibits are filed as part of this Annual Report on Form 10-K for the fiscal year ended December 31, 2006:

Exhibit	Description
2.1	Agreement and Plan of Merger, dated as of July 28, 2003, among Secure Computing Corporation, Nitro Acquisition Corp., and N2H2, Inc. is incorporated by reference to the corresponding exhibit to our Registration Statement of Form S-4 (Registration Number 333-107804) filed with the SEC on August 8, 2003.
2.2	Agreement and Plan of Merger, dated as of August 17, 2005, by and among Secure Computing Corporation, Bailey Acquisition Corp., and CyberGuard Corporation is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
2.3	Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on July 13, 2006.
2.4	First Amendment, dated July 14, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on July 18, 2006.

Table of Contents

Exhibit	Description
2.5	Second Amendment, dated August 1, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 2.1 to our Current Report on Form 8-K filed with the SEC on August 7, 2006.
2.6	Third Amendment, dated August 30, 2006, to the Agreement and Plan of Merger, dated as of July 11, 2006, by and among Secure Computing Corporation, Peach Acquisition Corp., and CipherTrust, Inc. is incorporated by reference to Exhibit 99.3 to our Current Report on Form 8-K filed with the SEC on September 28, 2006.
3.1	Restated Certificate of Incorporation, effective March 6, 1996, as amended by the Certificate of Amendment of Certificate of Incorporation effective December 11, 1988, the Certificate of Designations of Series E 4% Cumulative Preferred Stock effective January 26, 2000; and the Certificate of Designations of Series F 4% Cumulative Convertible Preferred Stock effective June 30, 2000 is incorporated by reference to the corresponding exhibit to our Amended Quarterly Report on Form 10-Q for the period ended June 30, 2000.
3.2	By-Laws of the Registrant are incorporated by reference to Exhibit 3.3 to our Registration Statement on Form S-1 (Registration Number 33-97838).
3.3	Certificate of Designations, Preferences and Rights of Series A Convertible Preferred Stock is incorporated by reference to Exhibit 3.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
4.1	Specimen of common stock certificate is incorporated by reference to the corresponding exhibit to Amendment No. 2 to our Registration Statement on Form S-1 (Registration Number 33-97838).
4.2	Amended and Restated 1995 Omnibus Stock Plan is incorporated by reference to the Exhibit 10.1 to our Current Report on Form 8-K filed on October 8, 1999.
4.3	2002 Stock Incentive Plan is incorporated by reference to Exhibit 99.1 to our Registration Statement on Form S-8 (Registration Number 333-115583) filed with the SEC on January 19, 2006.
4.4	CyberGuard Corporation Stock Incentive Plan is incorporated by reference to Exhibit 4.1 to CyberGuard Corporation's Registration Statement on Form S-8 (Registration Number 33-88448) filed with the SEC on January 13, 1995.
4.5	CyberGuard Corporation Third Amended and Restated Employee Stock Option Plan is incorporated by reference to CyberGuard Corporation's Proxy Statement filed on December 13, 2003.
4.6	Warrant by and among Secure Computing Corporation and Warburg Pincus IX, L.P. is incorporated by reference to Exhibit 4.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
4.7	CipherTrust, Inc. 2000 Stock Option Plan.
10.1	Employment Agreement with John McNulty is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended March 31, 1999.
10.2	Employment Agreement with Timothy Steinkopf is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended June 30, 2001.
10.3	Employment Agreement with Vince Schiavo is incorporated by reference to Exhibit 10.1 of our Quarterly Report of Form 10-Q for the period ended June 30, 2001.
10.4	Employment Agreement with Michael Gallagher is incorporated by reference to the corresponding exhibit of our Annual Report of Form 10-K for the period ended December 31, 2004.
10.5	Employment Agreement with Mary Budge is incorporated by reference to the corresponding exhibit of our Annual Report of Form 10-K for the period ended December 31, 2004.

Exhibit	Description
10.6	Securities Purchase Agreement, dated as of August 17, 2005, by and among Secure Computing Corporation and Warburg Pincus IX, L.P. is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on August 19, 2005.
10.7	Amendment No. 1 to the Securities Purchase Agreement by and among Secure Computing Corporation and Warburg Pincus IX, L.P. dated December 9, 2005 is incorporated by reference to Exhibit 99.1 to our Current Report on Form 8-K filed with the SEC on December 13, 2005.
10.8	Form of Indemnification Agreement between the Company, and Cary Davis dated January 31, 2006; Robert J. Frankenberg dated January 31, 2006; James Jordan dated February 1, 2006; John McNulty dated February 1, 2006; Stephen Puricelli dated January 31, 2006; Eric Rundquist dated January 31, 2006; Richard Scott dated January 31, 2006; and Alexander Zakupowsky, Jr. dated February 1, 2006 is incorporated by reference to Exhibit 10.6 to our Current Report on Form 8-K filed with the SEC on January 31, 2006.
10.9	Employment Agreement with Jay Chaudhry is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.10	Employment Agreement with Atri Chatterjee is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.11	Employment Agreement with Paul Judge is incorporated by reference to the corresponding exhibit of our Quarterly Report of Form 10-Q for the period ended September 30, 2006.
10.12	Senior Secured Credit Facilities Commitment Letter, dated as of July 11, 2006, from Citigroup, is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on July 13, 2006.
10.13	Amended and Restated Senior Secured Credit Facilities Commitment Letter, dated as of July 14, 2006, from Citigroup, is incorporated by reference to Exhibit 10.1 to our Current Report on Form 8-K filed with the SEC on July 18, 2006.
10.14	Form of Restricted Stock Award Agreement—Secure Computing Corporation 2002 Stock Incentive Plan.
23.1	Consent of Ernst & Young LLP.
24.1	Power of Attorney (See page 81)
31.1	Certification of Chief Executive Officer Pursuant to Section 302 of Sarbanes-Oxley Act of 2002.
31.2	Certification of Chief Financial Officer Pursuant to Section 302 of Sarbanes-Oxley Act of 2002.
32.1	Certification by Chairman, President and Chief Executive Officer Pursuant to Section 906 of Sarbanes-Oxley Act of 2002.
32.2	Certification by Senior Vice President and Chief Financial Officer Pursuant to Section 906 of Sarbanes-Oxley Act of 2002.

Table of Contents

SECURE COMPUTING CORPORATION
CONSOLIDATED BALANCE SHEETS
(in thousands, except share and per share amounts)

	December 31, 2006	December 31, 2005
ASSETS		
Current assets		
Cash and cash equivalents	$ 8,249	$ 50,039
Investments and restricted cash	457	31,140
Accounts receivable (net of reserves of 2006 - $1,427; 2005 - $272)	63,636	29,795
Inventory (net of reserves of 2006 - $472; 2005 - $264)	4,078	2,174
Deferred income taxes	—	3,604
Other current assets	13,948	4,869
Total current assets	90,368	121,621
Property and equipment		
Computer equipment and software	22,605	12,490
Furniture and fixtures	2,897	326
Leasehold improvements	2,795	1,093
	28,297	13,909
Accumulated depreciation	(13,997)	(10,068)
	14,300	3,841
Goodwill	533,659	39,230
Intangible assets (net of accumulated amortization of 2006 - $18,782; 2005 -$1,974)	78,388	1,814
Other assets	7,413	5,257
Total assets	$ 724,128	$ 171,763
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities		
Accounts payable	$ 12,442	$ 2,997
Accrued payroll	12,035	4,690
Accrued expenses	6,365	2,377
Acquisition reserves	1,418	389
Deferred revenue	86,612	29,097
Total current liabilities	118,872	39,550
Acquisition reserves, net of current portion	1,591	364
Deferred revenue, net of current portion	35,671	9,966
Deferred tax liability	7,672	—
Debt, net of fees	85,023	—
Total liabilities	248,829	49,880
Convertible preferred stock, par value $.01 per share: Authorized – 2,000,000 shares; issued and outstanding shares – December 31, 2006 – 700,000 and 2005 – none	65,558	—
Stockholders' equity		
Common stock, par value $.01 per share: Authorized – 100,000,000 shares; issued and outstanding shares – December 31, 2006 – 65,008,509 and December 31, 2005 – 37,021,089	651	370
Additional paid-in capital	538,616	205,970

Accumulated deficit	(127,249)	(83,698)
Accumulated other comprehensive loss	(2,277)	(759)
Total stockholders' equity	409,741	121,883
Total liabilities and stockholders' equity	$ 724,128	$ 171,763

See accompanying notes.

Table of Contents

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except share and per share amounts)

	Year Ended December 31,		
	2006	**2005**	**2004**
Revenue			
Products	$115,628	$ 79,339	$67,625
Services	61,069	29,836	25,753
Total revenues	176,697	109,175	93,378
Cost of revenues			
Products	31,540	16,876	12,335
Services	11,756	5,173	5,052
Amortization of purchased intangibles	5,862	—	—
Total cost of revenues	49,158	22,049	17,387
Gross profit	127,539	87,126	75,991
Operating expenses			
Selling and marketing	84,505	42,309	41,201
Research and development	34,073	16,781	16,106
General and administrative	13,608	7,189	6,456
Amortization of purchased intangibles	10,626	496	—
Litigation settlement	2,500	—	—
	145,312	66,775	63,763
Operating (loss)/income	(17,773)	20,351	12,228
Other (expense)/income	(120)	1,631	607
(Loss)/income before taxes	(17,893)	21,982	12,835
Income tax expense	(9,505)	(608)	—
Net (loss)/income	$ (27,398)	$ 21,374	$12,835
Preferred stock accretion	(3,550)	—	—
Charge from beneficial conversion of preferred stock	(12,603)	—	—
Net (loss)/income applicable to common shareholders	$ (43,551)	$ 21,374	$12,835
Basic (loss)/earnings per share	$ (0.76)	$ 0.59	$ 0.36
Weighted average shares outstanding - basic	57,010	36,338	35,576
Diluted (loss)/earnings per share	$ (0.76)	$ 0.57	$ 0.34
Weighted average shares outstanding - diluted	57,010	37,709	37,256

See accompanying notes.

Table of Contents

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY
(in thousands, except share amounts)

	Preferred Stock		Common Stock					
	Shares	Par Value	Shares	Par Value	Additional Paid-In Capital	Accumulated Deficit	Accumulated Other Comprehensive Loss	Total Stockholders' Equity
BALANCE, December 31, 2003	—	—	34,953,772	350	190,090	(117,907)	(519)	72,014
Comprehensive income:								
Net income for the year	—	—	—	—	—	12,835	—	12,835
Foreign currency translation adjustment	—	—	—	—	—		(183)	(183)
Unrealized loss on investments	—	—	—	—	—	—	(2)	(2)
Total comprehensive income								12,650
Exercise of employee stock options	—	—	678,451	6	5,787	—	—	5,793
Employee stock purchase plan activity	—	—	165,472	2	1,367	—	—	1,369
BALANCE, December 31, 2004	—	—	35,797,695	358	197,244	(105,072)	(704)	91,826
Comprehensive income:								
Net income for the year	—	—	—	—	—	21,374	—	21,374
Foreign currency translation adjustment	—	—	—	—	—	—	(61)	(61)
Unrealized gain on investments	—	—	—	—	—	—	6	6
Total comprehensive income								21,319
Exercise of employee stock options	—	—	1,059,050	10	7,364	—	—	7,374
Employee stock purchase plan activity	—	—	164,344	2	1,362	—	—	1,364
BALANCE, December 31, 2005	—	$ —	37,021,089	$ 370	$ 205,970	$ (83,698)	$ (759)	$ 121,883
Comprehensive loss:								
Net loss for the year	—	—	—	—	—	(27,398)	—	(27,398)
Foreign currency translation adjustment	—	—	—	—	—	—	(1,539)	(1,539)
Unrealized gain on investments	—	—	—	—	—	—	2	2
Unrealized gain on interest rate cap	—	—	—	—	—	—	19	19
Total comprehensive loss								(28,916)
Exercise of employee stock options	—	—	1,418,544	15	6,380	—	—	6,395
Employee stock purchase plan activity	—	—	278,706	3	1,746	—	—	1,749
Share-based compensation expense	—	—	—	—	10,556	—	—	10,556
Issuance of shares for CyberGuard acquisition	—	—	16,290,170	163	188,313	—	—	188,476
Fair value of CyberGuard options assumed in acquisition	—	—	—	—	29,326	—	—	29,326
Beneficial conversion charge for preferred stock	—	—	—	—	12,603	(12,603)	—	—
Preferred stock accretion	—	—	—	—	—	(3,550)	—	(3,550)
Issuance of warrants, net of fees	—	—	—	—	7,937	—	—	7,937
Issuance of shares for CipherTrust acquisition	—	—	10,000,000	100	68,000	—	—	68,100
Fair value of CipherTrust options assumed in acquisition	—	—	—	—	7,785	—	—	7,785
BALANCE, December 31, 2006	—	$ —	65,008,509	$ 651	$ 538,616	$ (127,249)	$ (2,277)	$ 409,741

See accompanying notes.

Table of Contents

SECURE COMPUTING CORPORATION
CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

	Year Ended December 31,		
	2006	2005	2004
Operating activities			
Net (loss)/income	$ (27,398)	$ 21,374	$ 12,835
Adjustments to reconcile net (loss)/income to net cash provided by operating activities:			
Depreciation	4,554	2,214	2,515
Amortization of intangible assets	17,011	881	887
Loss on disposals of property and equipment and intangible assets	999	486	48
Amortization of debt fees	155	—	—
Deferred income taxes	8,486	—	(345)
Share-based compensation	10,556	—	—
Changes in operating assets and liabilities, net of acquisitions:			
Accounts receivable	(12,112)	(9,532)	(2,795)
Inventory	161	621	(1,566)
Other current assets	(38)	619	(970)
Accounts payable	5,299	419	(133)
Accrued payroll	3,076	630	551
Accrued expenses	(4,263)	845	1,191
Acquisition reserves	(14,296)	(619)	(2,224)
Deferred revenue	43,933	9,616	4,006
Net cash provided by operating activities	36,123	27,554	14,000
Investing activities			
Proceeds from sales/maturities of investments	46,434	13,193	17,528
Purchases of investments	(15,406)	(29,921)	(10,355)
Purchase of property and equipment, net	(11,841)	(2,496)	(1,553)
Increase in intangibles and other assets	(1,785)	(4,867)	(802)
Cash paid for business acquisitions, net of cash acquired	(256,743)	—	—
Net cash (used in)/provided by investing activities	(239,341)	(24,091)	4,818
Financing activities			
Proceeds from revolving debt	8,500	—	—
Proceeds from term debt, net of fees	86,868	—	—
Proceeds from issuance of preferred stock and warrant, net of fees	69,945	—	—
Proceeds from issuance of common stock	8,144	8,738	7,162
Repayments of term and revolving debt	(10,500)	—	—
Net cash provided by investing activities	162,957	8,738	7,162
Effect of exchange rates	(1,529)	(61)	(182)
Net (decrease)/increase in cash and cash equivalents	(41,790)	12,140	25,798
Cash and cash equivalents, beginning of year	50,039	37,899	12,101
Cash and cash equivalents, end of year	$ 8,249	$ 50,039	$ 37,899
Supplemental Cash Flow Disclosures:			
Common stock issued for purchase of CyberGuard Corporation.	$ 188,476	—	—
Common stock issued for purchase of CipherTrust, Inc	$ 68,100	—	—

Interest paid	$ 2,711	—	—

See accompanying notes.

Table of Contents

SECURE COMPUTING CORPORATION
NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

1. Summary of Significant Accounting Policies

Organization

Secure Computing Corporation is a global leader in enterprise gateway security. Founded in 1989, we have been securing the connections between people and information for nearly 20 years. We use our broad expertise in security technology to develop enterprise gateway security solutions that allow organizations to exchange critical information safely with their customers, partners and employees using trusted connections. Specializing in delivering enterprise-class solutions that secure Web, email, and network connectivity, we are proud to be the global security solutions provider to some of the most mission-critical network environments in the world.

Basis of Consolidation

The consolidated financial statements include the accounts of Secure Computing and our wholly-owned subsidiaries. All intercompany balances and transactions have been eliminated in consolidation.

Use of Estimates

The preparation of financial statements in conformity with U.S. generally accepted accounting principles requires management to make estimates and assumptions that affect the amounts reported in the financial statements and accompanying notes. Actual results could differ from those estimates.

Revenue Recognition

We derive our revenue primarily from two sources: (i) sales of products, including hardware, subscriptions, software licenses, and royalties and (ii) sales of services, including maintenance arrangements to provide upgrades and customer support, professional services, and contracted development work. We recognize revenue in accordance with Statement of Position (SOP) 97-2, "Software Revenue Recognition," as modified by SOP 98-9. Revenue from products is recognized when persuasive evidence of an arrangement exists, delivery has occurred, the fee is fixed and determinable, and collection is probable. Subscription-based contracts are generally for 12, 24 or 36 months in duration. Subscription revenue along with maintenance revenue for providing product upgrades and customer support are deferred and recognized ratably over the service period beginning with the month the subscription or service begins.

When arrangements contain multiple elements and vendor specific objective evidence (VSOE) of fair value exists for all undelivered elements, we recognize revenue for the delivered elements using the residual method. For arrangements containing multiple elements where VSOE of fair value does not exist for all undelivered elements, we defer revenue for the delivered and undelivered elements and then recognize revenue on all elements over the service period. In instances where an entire arrangement is deferred due to lack of VSOE of fair value on an undelivered element, the revenue recognized over the service period is allocated to products and services revenue based on the value of the elements as presented on the customer's purchase order which approximates an allocation proportionate to our list price. We also identify costs (primarily hardware component costs) that are directly associated with product revenues that have been deferred due to lack of VSOE of fair value on an undelivered element and we defer these costs at the time of shipment and recognize them as cost of sales in proportion to the product revenue as it is recognized over the service term.

We sell our products either directly to an end-user, or indirectly through our channel of resellers and distributors (our channel partners). When selling through our channel we require our channel partners to provide evidence of end-user sell-through. If we are unable to obtain end-user evidence at the time we fulfill the order from a channel partner, we do not recognize revenue until the channel partner supplies end-user information, the product has been shipped, and all other criteria of SOP 97-2 have been met, with the exception of sales to our distributors who stock our SnapGear product line. We recognize revenue, net of estimated returns, upon shipment of our SnapGear product line as we have sufficient return history to establish a reserve and we are not able to receive end-user evidence due to the high-volume sales of this low-price point product.

Cash Equivalents and Short-Term Investments

We account for investments with the provisions of Statement of Financial Accounting Standards (SFAS) No. 115, "Accounting for Certain Investments in Debt and Equity Securities." SFAS No. 115 addresses the accounting and reporting for investments in fixed maturity securities and for equity securities with readily determinable fair values. Our short-term investments do not include strategic investments. All of our short-term investments are classified as available-for-sale and consist of securities with original maturities in excess of 90 days. We consider investments in instruments purchased with an original maturity of 90 days or less to be cash equivalents. Cash equivalents are carried at cost, which approximates fair value. Short-term investments are carried at fair value as determined by quoted market prices, with unrealized gains and losses, net of tax, reported as a separate component of stockholders' equity. The cost basis of investments that are sold or matured is determined using the specific identification method. Interest and dividends on investments classified as available-for-sale, amortization of premiums and discounts on investments and realized gains and losses and declines in fair value judged to be other-than-temporary on available-for-sale securities are included in other (expense)/income on the consolidated statements of operations. The gross realized gains and losses for the sale or maturity of available-for-sale investments are not material in all periods presented.

Derivative Instrument

In September 2006, we entered into an interest rate cap agreement which is required to be accounted for under SFAS No. 133, "Accounting for Derivative Instruments and Hedging Activities." SFAS No. 133 establishes accounting and reporting standards for derivative instruments, including certain derivative instruments embedded in other contracts, and for hedging activities. It requires that an entity recognize all derivatives as either assets or liabilities in the statement of financial position and measure those instruments at fair value. If certain conditions are met, a derivative may be specifically designated as (a) a hedge of the exposure to changes in the fair value of a recognized asset or liability or an unrecognized firm commitment, (b) a hedge of the exposure to variable cash flows of a forecasted transaction, or (c) a hedge of the foreign currency exposure of a net investment in a foreign operation, an unrecognized firm commitment, an available-for-sale security, or a foreign-currency-denominated forecasted transaction. The interest rate cap agreement applies to (b), referred to as a cash flow hedge. For a derivative that is designated as a cash flow hedge the effective portion of the derivative's gain or loss is initially reported as a component of other comprehensive income or loss (see "Comprehensive (Loss)/Income" below) and subsequently reclassified into earnings when the forecasted transaction affects earnings. The ineffective portion of the gain or loss is immediately recognized in income.

Accounts Receivable

Accounts receivable are initially recorded at fair value upon the sale of products or services to our customers. We make estimates regarding the collectibility of our accounts receivables which we use to record a provision for doubtful accounts. When we evaluate the adequacy of our allowance for doubtful accounts, we consider multiple factors including historical write-off experience, the need for specific customer reserves, the aging of our receivables, customer creditworthiness, changes in our customer payment cycles, and current economic trends. The provision for doubtful accounts is included in selling and marketing expense on the consolidated statement of operations. If the financial condition of our customers were to deteriorate, resulting in an impairment of their ability to make payments, additional allowances may be required.

Table of Contents

Equity Investments

We have an equity investment in a privately held company for business and strategic purposes. This investment is included in other assets on our consolidated balance sheets and is accounted for under the cost method as we do not have significant influence over the investee. Under the cost method, the investment is recorded at its initial cost and is periodically reviewed for impairment. Each quarter we assess our compliance with accounting guidance, including the provisions of Financial Accounting Standards Board Interpretation No. (FIN) 46R, "Consolidation of Variable Interest Entities—An Interpretation of ARB No. 51", and any impairment issues. Under FIN 46R, we must consolidate a variable interest entity if we have a variable interest (or combination of variable interests) in the entity that will absorb a majority of the entity's expected losses, receive a majority of the entity's expected residual returns, or both. Currently, our equity investment is not subject to consolidation under FIN 46R as we do not have significant influence over this investee and we do not receive a majority of the returns. During our review for impairment, we examine the investees' actual and forecasted operating results, financial position, and liquidity, as well as business/industry factors in assessing whether a decline in value of an equity investment has occurred that is other-than-temporary. When such a decline in value is identified, the fair value of the equity investment is estimated based on the preceding factors and an impairment loss is recognized in interest and other (expense)/income, in the consolidated statements of operations. During the years ended December 31, 2006 and 2005, we did not recognize an impairment loss on our equity investment.

Inventories

Inventories consist mainly of purchased components and prepaid licenses and are valued at the lower of cost or market using the first-in, first-out (FIFO) method.

Property and Equipment

Property and equipment are carried at cost. Depreciation is calculated using the straight-line method. Estimated useful lives are 3 years for computer equipment and software and 7 years for furniture and fixtures. Leasehold improvements are depreciated over the lesser of the useful life of the asset or the term of the lease.

Financial Instruments

Carrying amounts of financial instruments held by us, which include cash equivalents, short-term investments, restricted cash, accounts receivable, accounts payable and accrued expenses, approximate fair value due to their short-term nature. In the case of our long-term debt, the carrying value of the debt approximates its fair value due to the fact that it is variable-rate debt that reprices frequently. In addition, our credit standing has not changed significantly.

Other Current Assets and Other Assets

Other current assets are carried at cost and consist of unbilled receivables, interest receivable, a derivative instrument, deferred cost of goods sold and prepaid expenses for items such as directors and officers liability insurance, trade shows, royalties, inventory components and foreign taxes to be either expensed or collected within 12 months. Other assets are carried at cost and include a strategic equity investment (see Note 16), rent deposits, and deferred cost of goods sold to be collected or expensed after 12 months.

Income Taxes

We account for income taxes under SFAS No. 109, "Accounting for Income Taxes," which requires recognition of deferred tax liabilities and assets for the expected future tax consequences of events that have been included in our financial statements or tax returns. Under this method, deferred tax liabilities and assets are determined based on the difference between the financial statement and tax basis of assets and liabilities, using enacted tax rates in effect for the year in which the differences are expected to reverse. SFAS No. 109 requires the consideration of a valuation allowance for deferred tax assets if it is "more likely than not" that some component or all of the benefits of deferred tax assets will not be realized.

Goodwill and Other Intangible Assets

Intangible assets consist of patents, trademarks, capitalized software costs, purchased customer and control lists, purchased tradenames, capitalized developed technology and goodwill, all of which are recorded at cost or fair value. Patents, trademarks, tradenames, control lists, and capitalized developed technology are amortized using the straight-line method over the estimated useful lives of the assets, which range up to 17 years. Customer lists are amortized on an accelerated basis based on an attrition rate driven by the estimated revenue stream from acquired customers over a five year period. See accounting policy of capitalized software costs below under Research and Development.

Goodwill is not amortized, but is tested for impairment at the reporting unit level at least annually. If impairment is indicated, a write-down is recorded as an impairment loss in income from operations. An impairment charge is recognized only when the calculated fair value of a reporting unit, including goodwill, is less than its carrying amount. In accordance with SFAS No. 142, "Goodwill and Other Intangible Assets," we completed the required annual impairment tests of goodwill during the fourth quarter of 2006 and 2005 and determined the fair value to be in excess of the carrying value of these assets. Therefore, goodwill was not impaired and no impairment charge was reported.

Long-Lived Assets

We review our long-lived assets and identified finite-lived intangible assets for impairment whenever events or changes in circumstances indicate that the carrying amount of an asset may not be recoverable, except for goodwill as noted above. Recoverability of assets to be held and used is measured by a comparison of the carrying amount of an asset to undiscounted future net cash flows expected to be generated by the assets. If such assets are considered to be impaired, the impairment to be recognized is measured by the amount by which the carrying amount of the assets exceeds the fair value of the assets. There were no such impairments during the periods presented.

Accrued Expenses

At December 31, 2006 and 2005, accrued expenses consisted of costs related to professional fees, royalties, foreign taxes and accrued marketing development funds.

Leases and Deferred Rent

We lease all of our office space. Leases are accounted for under the provisions of SFAS No. 13, "Accounting for Leases," as amended, which requires that leases be evaluated and classified as operating or capital leases for financial reporting purposes. As of December 31, 2006, all of our leases were accounted for as operating leases. For leases that contain rent escalations, we record the total rent payable during the lease term, as determined above, on a straight-line basis over the term of the lease and record the difference between the rents paid and the straight-line rent as a deferred rent.

Concentrations of Credit Risk

Financial instruments that potentially subject us to concentrations of credit risk consist primarily of accounts receivable. We perform ongoing credit evaluations of our customers, generally require customers to prepay for maintenance and maintain reserves for potential losses. Our customer base is primarily composed of businesses throughout the U.S., Europe, Japan, China, the Pacific Rim, and Latin America.

Table of Contents

Interest Rate Risk

We have market risk exposure to changing interest rates primarily as a result of our borrowing activities. Our objective in managing our exposure to changes in interest rates is to reduce fluctuations in earnings and cash flows. To achieve these objectives, we use derivative instruments, such as our interest rate cap agreement, to manage risk exposures when appropriate, based on market conditions. We do not enter into derivative agreements for trading or other speculative purposes, nor are we a party to any leveraged derivative instrument.

Foreign Currency Translation and Transactions

Foreign assets and liabilities were translated using the exchange rates in effect at the balance sheet date. Results of operations were translated using average exchange rates throughout the year. Translation gains or losses have been reported in other comprehensive (loss)/income as a component of stockholders' equity. Cumulative foreign currency translation loss balances were $2.3 million and $757,000 at December 31, 2006 and 2005, respectively. Any gains or losses resulting from foreign currency transactions are included in the consolidated statements of operations and are not significant during the periods presented.

Comprehensive (Loss)/Income

The components of our comprehensive (loss)/income are net (loss)/income, foreign currency translation adjustments, unrealized gain on investments and unrealized gain on our interest rate hedge. Comprehensive (loss)/income for all periods presented is included in our consolidated statements of stockholders' equity.

Selling and Marketing

Selling and marketing expenses consist primarily of salaries, commissions, share-based compensation and benefits related to personnel engaged in selling and marketing functions, along with costs related to advertising, promotions, and public relations. Our customer support function, which provides support, training and installation services, is also responsible for supporting our sales representatives and sales engineers throughout the sales cycle by providing them and our prospective customers with technical assistance and, as such, a portion of these costs are included as selling and marketing expense.

Research and Development

Research and development expenditures are charged to operations as incurred. SFAS No. 86, "Accounting for the Costs of Computer Software to Be Sold, Leased, or Otherwise Marketed," requires capitalization of certain software development costs subsequent to the establishment of technological feasibility. Based on our product development process, technological feasibility is established upon completion of a working model. Costs that we incur between completion of the working model and the point at which the product is generally available for sale are capitalized and amortized over their estimated useful life of three years.

Share-Based Compensation

Prior to January 1, 2006, we accounted for share-based employee compensation plans under the measurement and recognition provisions of Accounting Principles Board (APB) Opinion No. 25, "Accounting for Stock Issued to Employees," and related Interpretations, as permitted by SFAS No. 123, "Accounting for Stock-Based Compensation." Accordingly, we recorded no share-based employee compensation expense for options granted under our current stock option plans during the year ended December 31, 2005 as all options granted under those plans had exercise prices equal to the fair market value of our common stock on the date of grant. We also recorded no compensation expense in those periods in connection with our Employee Stock Purchase Plan (ESPP) as the purchase price of the stock was not less than 85% of the lower of the fair market value of our common stock at the beginning of each offering period or at the end of each purchase period. In accordance with SFAS No. 123 and SFAS No. 148, "Accounting for Stock-Based Compensation – Transition and Disclosure," we provided pro forma net income or loss and net income or loss per share disclosures for each period prior to the adoption of SFAS No. 123(R), "Share-Based Payment," as if we had applied the fair value-based method in measuring compensation expense for our share-based compensation plans.

Effective January 1, 2006, we adopted the fair value recognition provisions of SFAS No. 123(R), using the modified prospective transition method. Under that transition method, we recognized compensation expense for share-based payments that vested during 2006 using the following valuation methods: (a) for share-based payments granted prior to, but not yet vested as of, January 1, 2006, the grant date fair value was estimated in accordance with the original provisions of SFAS No. 123, and (b) for share-based payments granted on or after January 1, 2006, the grant date fair value was estimated in accordance with the provisions of SFAS No. 123(R). Because we elected to use the modified prospective transition method, results for prior periods have not been restated. In March 2005, the Securities and Exchange Commission issued Staff Accounting Bulletin (SAB) No. 107, "Share-Based Payment," which provides supplemental implementation guidance for SFAS No. 123(R). We have applied the provisions of SAB No. 107 in our adoption of SFAS No. 123(R). See Note 10 for information on the impact of our adoption of SFAS No. 123(R) and the assumptions we use to calculate the fair value of share-based compensation.

Net (Loss)/Income Per Share

In accordance with SFAS No. 128, "Earnings Per Share," basic net (loss)/income per share is computed by dividing net (loss)/income applicable to common shareholders by the weighted average number of common shares outstanding during the period. Diluted net loss per share is computed by dividing net loss applicable to common shareholders by the weighted average number of common shares outstanding during the period. Diluted net income per share is computed by dividing net income by the combination of dilutive common share equivalents, which consist of stock options and the weighted average number of common shares outstanding.

Recently Issued Accounting Standards

In July 2006, the FASB issued Interpretation No. 48 (FIN 48), "Accounting for Uncertainty in Income Taxes, an Interpretation of SFAS No. 109." FIN 48 creates a single model to address accounting for uncertainty in tax positions and clarifies the accounting for income taxes by prescribing the minimum recognition threshold a tax position is required to meet before being recognized in the financial statements. Specifically under FIN 48, the tax benefits from an uncertain tax position may be recognized only if it is more likely than not that the tax position will be sustained on examination by the taxing authorities, based upon the technical merits of the position. FIN 48 also provides guidance on de-recognition, measurement, classification, interest and penalties, accounting in interim periods, disclosure and transition. FIN 48 is effective for fiscal years beginning after December 15, 2006. As prescribed in the interpretation, the cumulative effect of applying the provisions of FIN 48 will be reported as an adjustment to the opening balance of retained earnings at January 1, 2007. We will adopt FIN 48 effective January 1, 2007 as required. We are currently evaluating the potential impact which the adoption of FIN 48 will have on our financial position, cash flows, and results of operations.

In September 2006, the FASB issued SFAS No. 157, "Fair Value Measurements." SFAS No. 157 establishes a framework for measuring fair value in generally accepted accounting principles, clarifies the definition of fair value within that framework, and expands disclosures about the use of fair value measurements. SFAS No. 157 is intended to increase consistency and comparability among fair value estimates used in financial reporting. As such, SFAS No. 157 applies to all other accounting pronouncements that require (or permit) fair value measurements, except for the measurement of share-based payments. SFAS No. 157 does not apply to accounting standards that require (or permit) measurements that are similar to, but not intended to represent, fair value. Fair value, as defined in SFAS No. 157, is the price to sell an asset or transfer a liability and therefore represents an exit price, not an entry price. The exit price is the price in the principal market in which the reporting entity would transact. Further, that price is not adjusted for transaction costs. SFAS No. 157 is effective for fiscal years beginning after November 15, 2007, and interim periods within those fiscal years. SFAS No. 157 will be applied prospectively as of the beginning of the fiscal year in which it is initially applied. We are currently assessing the impact of adoption of SFAS No. 157.

2. Acquisition of CipherTrust

On August 31, 2006, we acquired 100% of the outstanding common shares of CipherTrust, Inc., a privately-held company. CipherTrust's products provide innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions and phishing, and protect against outbound policy and compliance violations associated with sensitive data leakage. CipherTrust's products include IronMail, powered by TrustedSource, IronIM, IronMail Edge, IronNet, and RADAR. As a result of the acquisition we expect to establish ourselves as a leader in the Messaging Gateway Security market. In addition to protecting corporate network infrastructures, our combined solutions will address the fast-growing Web and Messaging Gateway Security needs.

The aggregate purchase price was $270.1 million consisting primarily of $188.1 million in cash, the issuance of 10.0 million shares of common stock valued at $68.1 million, the conversion of outstanding CipherTrust stock options into options to purchase 2.5 million shares of our common stock with a fair value of $7.8 million, and direct costs of the acquisition of $6.1 million. The value of the common shares issued was determined based on the average market price of our common shares over the period including two days before and two days after the date that the terms of the acquisition were agreed to and announced. We financed $90.0 million of the CipherTrust acquisition through debt financing obtained from a syndicate of banks led by Citigroup and UBS Investment Bank. See Note 6 for details on the debt financing. As part of the terms of the acquisition, we may issue a $10.0 million note to former CipherTrust shareholders that is subject to the attainment of certain performance conditions to be met by September 30, 2007. Any contingent consideration earned will be recorded as additional goodwill.

The acquisition was accounted for under the purchase method of accounting, and accordingly, the assets and liabilities acquired were recorded at their estimated fair values at the effective date of the acquisition and the results of operations have been included in the consolidated statements of operations since the acquisition date. In accordance with SFAS No. 142, "Goodwill and Other Intangible Assets," goodwill and indefinite lived trademarks recorded as a result of the acquisition will be subject to an annual impairment test and will not be amortized.

Table of Contents

The following table summarizes the estimated preliminary fair values of the assets acquired and liabilities assumed at the date of acquisition (in thousands):

		As of August 31, 2006
Cash paid, net of cash acquired		$ (187,647)
Current assets		11,399
Property and equipment		1,474
Other long-term assets and indefinite lived assets		8,153
Goodwill		233,857
Intangible assets subject to amortization:		
Intangibles – Customer relationships (60 month useful life)	14,298	
Intangibles – Developed technology (48 month useful life)	21,445	
		35,743
Total assets acquired		102,979
Current liabilities		6,853
Acquisition reserve		7,194
Revenue deferred from ongoing contractual obligations at fair value		10,384
Deferred tax liability – long-term		2,663
Fair value of assets and liabilities assumed and accrued, net		$ 75,885

We accrued $7.2 million in acquisition related expenses, which included legal and accounting fees, bankers' fees, severance costs and other related costs, of which $342,000, related to severance costs and legal, accounting and tax fees, remains as an accrual as of December 31, 2006.

The following table presents our consolidated results of operations on an unaudited proforma basis as if the acquisitions had taken place at the beginning of the periods presented (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Total revenues	$211,746	$154,591	$130,819
Net loss applicable to common shareholders	(62,900)	(6,732)	(5,018)
Basic and diluted loss per share	$ (0.99)	$ (0.15)	$ (0.11)

The unaudited pro forma data gives effect to actual operating results prior to the acquisitions, and adjustments to reflect interest income foregone, increased intangible amortization, and interest expense for debt assumed. No effect has been given to cost reductions or operating synergies in this presentation. As a result, the unaudited pro forma results of operations are for comparative purposes only and are not necessarily indicative of the results that would have been obtained if the acquisition had occurred as of the beginning of the periods presented or that may occur in the future.

3. Acquisition of CyberGuard

On January 12, 2006, we acquired 100% of the outstanding common shares of CyberGuard Corporation. CyberGuard provided network security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communication. CyberGuard's products included firewall, Virtual Private Network (VPN), secure content management and security management technologies. This acquisition strengthens our position as one of the market leaders in Network Gateway Security and strengthens our position in the Web Gateway Security space. Additionally, we now have a larger presence in the Global 5000 enterprise markets as well as the U.S. federal government.

The aggregate purchase price was $310.7 million consisting of the issuance of 16.3 million shares of common stock valued at $188.5 million, $2.73 in cash issued for each outstanding share of CyberGuard common stock valued at $88.9 million, the conversion of outstanding CyberGuard stock options into options to purchase 3.0 million shares of our common stock with a value of $29.3 million and direct costs of the acquisition of $4.0 million. The value of the common shares issued was determined based on the average market price of our common shares over the period including two days before and two days after the date that the terms of the acquisition were agreed to and announced. We financed $70.0 million of the CyberGuard acquisition through the issuance of preferred equity securities. See Note 7 for details on the equity financing.

The acquisition was accounted for under the purchase method of accounting, and accordingly, the assets and liabilities acquired were recorded at their estimated fair values at the effective date of the acquisition and the results of operations have been included in the consolidated statements of operations since the acquisition date. In accordance with SFAS No. 142, goodwill and indefinite lived trademarks recorded as a result of the acquisition will be subject to an annual impairment test and will not be amortized.

The following table summarizes the preliminary fair values of the assets acquired and liabilities assumed at the date of acquisition (in thousands):

		As of January 12, 2006
Cash paid, net of cash acquired		$ (69,096)
Current assets		18,067
Property and equipment		2,090
Other long-term and indefinite lived assets		10,570
Goodwill		268,314
Intangible assets subject to amortization:		
Customer relationships (60 month useful life)	28,610	
Tradenames (6 month useful life)	390	
Tradenames (12 month useful life)	290	
Acquired developed technology (12 month useful life)	2,080	
Acquired developed technology (36 month useful life)	1,160	
Acquired developed technology (48 month useful life)	6,930	
		39,460
Total assets acquired		269,405
Current liabilities		9,325
Acquisition reserve		9,358
Revenue deferred from ongoing contractual obligations at fair value		28,903
Deferred tax liability – long-term		4,017
Fair value of assets and liabilities assumed and accrued, net		$ 217,802

We accrued $9.4 million in acquisition related expenses, which included legal and accounting fees, excess capacity costs, directors and officers insurance policy premium, bankers' fees, severance costs and other costs of which $2.0 remains as an accrual as of December 31, 2006.

Table of Contents

The following table presents our consolidated results of operations on an unaudited proforma basis as if the acquisitions had taken place at the beginning of the periods presented (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Total revenues	$178,474	$167,775	$153,118
Net (loss)/income	(27,377)	7,850	1,110
Net (loss)/income applicable to common shareholders	(30,927)	4,197	(2,552)
Basic (loss)/earnings per share	$ (0.54)	$ 0.08	$ (0.05)
Diluted (loss)/earnings per share	$ (0.54)	$ 0.15	$ (0.05)

The unaudited pro forma data gives effect to actual operating results prior to the acquisitions, and adjustments to reflect interest income foregone, increased intangible amortization, income taxes, and preferred stock accretion. No effect has been given to cost reductions or operating synergies in this presentation. As a result, the unaudited pro forma results of operations are for comparative purposes only and are not necessarily indicative of the results that would have been obtained if the acquisition had occurred as of the beginning of the periods presented or that may occur in the future.

4. Investments

Cash Equivalents, Short-Term Investments and Restricted Cash

Our cash equivalents, short-term investments and restricted cash were as follows (in thousands):

	As of December 31,	
	2006	2005
Money market funds	$ 42	$ 32,998
Variable rate demand note	—	4,210
Commercial paper	—	12,920
Federal agencies	—	999
U.S. treasury bills	—	3,963
Taxable auction rate securities	—	22,950
Certificates of deposit	218	245
Total investments	260	78,285
Amounts classified as cash equivalents	—	(47,145)
Restricted cash set aside in bank account	197	—
Total short-term investments and restricted cash	$457	$ 31,140

All short-term investments are debt securities and mature within one year. Unrealized losses on available-for-sale investments at December 31, 2006 and 2005 were none and $2,000, respectively and are reported as a component of other comprehensive (loss)/income in the statement of stockholders' equity. We have restricted cash pledged in the form of certificates of deposit and money market funds against our letters of credit of $205,000 and $40,000, respectively, at December 31, 2006 and in the form of certificates of deposit and money market funds of $240,000 and $40,000, respectively, at December 31, 2005. Interest income on cash equivalents, short-term investments and restricted cash was $2.7 million in 2006, prior to the liquidation of investments and cash equivalents to finance the CipherTrust acquisition, and $1.9 million in 2005.

Table of Contents

Equity Investment in a Privately Held Company

As of December 31, 2006, we held an equity investment with a carrying value of $2.7 million in a privately-held company. This investment was recorded at cost as we do not have significant influence over the investee and is classified as other assets on our consolidated balance sheets. This was a related party transaction as discussed in Note 16.

5. Goodwill and Other Intangible Assets

The changes in goodwill during 2006 and 2005 were as follows (in thousands):

Balance as of December 31, 2004	$ 39,329
Reversal of N2H2 reserves	(99)
Balance as of December 31, 2005	$ 39,230
Addition due to CyberGuard acquisition	268,314
Addition due to CipherTrust acquisition	233,857
Recognition of acquired deferred tax assets	(7,742)
Balance as of December 31, 2006	$533,659

As of December 31, 2006, indefinite lived tradenames related to the CipherTrust and CyberGuard acquisitions were $6.9 million and $10.5 million, respectively.

Identified intangible assets subject to amortization are as follows (in thousands):

	As of December 31, 2006			As of December 31, 2005		
	Carrying Value	Accumulated Amortization	Net	Carrying Value	Accumulated Amortization	Net
Customer lists	$44,049	$ (10,795)	$33,254	$ 1,141	$ (840)	$ 301
Tradenames	680	(671)	9	—	—	—
Control lists	771	(660)	111	771	(493)	278
Capitalized developed technology	31,657	(5,904)	25,753	42	(42)	—
Patents and trademarks	1,665	(502)	1,163	1,382	(340)	1,042
Capitalized software	953	(250)	703	452	(259)	193
Total	$79,775	$ (18,782)	$60,993	$ 3,788	$ (1,974)	$1,814

Total amortization expense was $17.0 million, $881,000 and $887,000 for the years ended December 31, 2006, 2005 and 2004, respectively. Of the total amortization expense, $187,000, $156,000, and $219,000 pertained to capitalized software costs for the years ended December 31, 2006, 2005, and 2004. Estimated amortization expense for each of the five succeeding fiscal years based on current intangible assets is expected to be $19.1 million, $16.7 million, $14.8 million, $9.1 million and $1.3 million, respectively.

6. Debt

Debt as of December 31, 2006 consists of the following (in thousands):

Secured term loan, due August 31, 2013, LIBOR plus 3.25%	88,000
Deferred financing fees related to secured term loan, due August 31, 2013	(2,977)
Total debt	$85,023

Table of Contents

Senior Secured Credit Facility

On August 31, 2006, we entered into a senior secured credit facility with a syndicate of banks led by Citigroup and UBS Investment Bank. The credit facility provides for a $90.0 million term loan facility, a $20.0 million revolving credit facility, and a swingline loan sub-facility. The proceeds from this transaction were used to finance a portion of the CipherTrust acquisition as noted in Note 2 above. The term loan matures on August 31, 2013 and is payable in 27 scheduled quarterly installments of $225,000 beginning in December 2006 with a final payment of $83.9 million due at maturity. Interest is payable quarterly on the term loan at the London Interbank Offered Rate ("LIBOR") + 3.25%. The interest rate on the term loan may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +3.00%. The interest rate in effect as of December 31, 2006 was 8.62%. Including amortization of deferred financing fees, we incurred $2.9 million of interest expense in 2006 and none in 2005. Our future payment obligations under this credit facility, are as follows (in thousands):

		Payments Due by Period			
	Total	Less Than One Year	One to Three Years	Three to Five Years	After Five Years
Principal payments on debt	$ 88,000	$ —	$ 925	$ 1,800	$85,275
Interest payments on debt	50,509	7,730	15,365	15,077	12,337
Total	$138,509	$ 7,730	$ 16,290	$ 16,877	$97,612

The revolving credit facility matures on August 31, 2012 with interest payable quarterly at LIBOR + 3.25%. The interest rate on the revolving credit facility may be adjusted quarterly based on our Leverage Ratio and range from LIBOR +3.25% to LIBOR +2.75%. The revolving credit facility also requires that we pay an annual commitment fee of .5%. The annual commitment fee, based on our Leverage Ratio and ranging from .5% to .375%, is payable quarterly in arrears. The Leverage Ratio is defined as the ratio of (a) consolidated indebtedness to (b) consolidated adjusted EBITDA (earnings before interest, taxes, depreciation, amortization and other adjustments as defined in the agreement). The Leverage Ratio will be calculated quarterly on a pro forma basis that includes the four preceding quarters. The initial Leverage Ratio calculation will be as of December 31, 2006 and cannot exceed the following thresholds over the term of the loan: August 31, 2006 through December 31, 2006 – 4.75 to 1.00; First six months of Fiscal 2007 – 4.00 to 1.00; Last six months of Fiscal 2007 – 3.50 to 1.00; Fiscal 2008 – 2.50 to 1.0; Fiscal 2009 – 2.25 to 1.00; Fiscal 2010 through maturity – 2.00 to 1.00.

The obligations under the senior secured credit facility are guaranteed by us and are secured by a perfected security interest in substantially all of our assets. Financing fees incurred in connection with the credit facility were deferred and are included as a reduction to our long-term debt. These fees are being amortized to interest expense over the term of the term loan using the effective interest rate method.

Debt Covenants

The credit facility agreement contains various covenants including limitations on additional indebtedness, capital expenditures, restricted payments, the incurrence of liens, transactions with affiliates and sales of assets. In addition, the credit facility requires us to comply with certain quarterly financial covenants, beginning with the quarter ended December 31, 2006, including maintaining leverage and interest coverage ratios and capital expenditure limitations. We are in compliance with all covenants as of December 31, 2006.

Derivative Instrument

We have entered into a 3-month LIBOR interest rate cap agreement to cap the interest rate at 5.5% on $60.0 million, or approximately 67% of the aggregate term loan. The notional amount of the agreement decreases $10.0 million each quarter starting March 30, 2007. The agreement terminates on June 30, 2008. The interest rate cap agreement is designated as a cash flow hedge and is reflected at fair value in our consolidated balance sheet. The related gains or losses on this contract are reflected in stockholders' equity as a component of other comprehensive (loss)/income. However, to the extent that this contract is not considered to be perfectly effective in offsetting the change in the value of the item being hedged, any change in fair value relating to the ineffective portion of this contract will be immediately recognized in income. The unrealized gain on the interest rate cap agreement is $19,000 as of December 31, 2006.

7. Equity Financing

On January 12, 2006, we received from Warburg Pincus Private Equity IX, L.P., a global private equity fund, $70.0 million in gross proceeds from the issuance of 700,000 of Series A Convertible Preferred Stock (the preferred stock), a warrant to acquire 1.0 million shares of our common stock and election of a member to our Board of Directors. Based on a quoted market price as of January 12, 2006 and the fair value of the warrant as determined using the Black-Scholes model, we valued the preferred stock at $62.0 million and the warrant at $8.0 million. The proceeds from this transaction were used to finance most of the cash portion of the CyberGuard acquisition as noted in Note 3 above.

On August 31, 2006, the conversion price for the preferred stock was adjusted from the original price of $13.51 to $12.75 per share in accordance with an anti-dilution adjustment triggered by the CipherTrust acquisition. Holders of our preferred stock will be entitled to receive benefits not available to holders of our common stock. These benefits include, but are not limited to, the following: beginning in July 2010, shares of preferred stock will be entitled to receive semi-annual dividends, which may be paid in cash or added to the preferred stock liquidation preference equal to 5% of the preferred stock liquidation preference per year and each share of preferred stock has an initial liquidation preference of $100 which accretes daily at an annual rate of 5%, compounded semi-annually, until July 2010.

On August 31, 2006, the exercise price for the warrant was adjusted from the original price of $14.74 to $13.85 per share also in accordance with an anti-dilution adjustment triggered by the CipherTrust acquisition. The warrant expires on January 12, 2013. When the market price of our common stock is above their exercise price, the warrant becomes dilutive and 1.0 million shares are immediately included in the computation of diluted earnings per share as if the warrant is exercised using the treasury stock method.

The preferred stock was initially reflected on our financial statements at $62.0 million, which is a discount of $8.0 million from its initial liquidation value of $70.0 million due to the fair value of warrants on the effective date. The liquidation value of the preferred stock accretes daily at an annual rate of 5%, compounded semi-annually. This accretion is recorded as a reduction of earnings attributable to common shareholders ratably for a period of 54 months after date of issuance.

We incurred a beneficial conversion charge of $12.6 million, which was recorded as a reduction in earnings attributable to common shareholders in 2006, upon the issuance of the preferred stock since the effective conversion price, after adjusting for the value of the warrants, was less than market price on January 12, 2006, the date of issuance. However, in August 2005 when the terms of the preferred stock issuance to Warburg Pincus in the Securities Purchase Agreement were negotiated, the average market price of the common stock was, in fact, less than the conversion price.

8. Letters of Credit

As of December 31, 2006, we have three letter of credit agreements totaling $247,000. One letter of credit for $205,000 and $240,000, as of December 31, 2006 and 2005, respectively, is with a bank to secure rental space for our San Jose, CA office and automatically renews for a one year period each year through March 31, 2008. Two remaining letters of credit totaling $42,000 and $40,000 as of December 31, 2006 and 2005, respectively, are to secure business with an international customer, which expire May and August 2008.

Table of Contents

9. Leases

We lease office space for all of our locations. Renewal options exist for our Concord, CA, and St. Paul, MN offices. Future lease payments for all operating leases, excluding executory costs such as management and maintenance fees and property tax, are as follows (in thousands):

	Future Lease Obligations	Sublease	Net Future Lease Obligations
2007	$ 5,474	$ (210)	$ 5,264
2008	4,381	(210)	4,171
2009	3,371	(122)	3,249
2010	2,238	—	2,238
2011	1,957	—	1,957
Thereafter	6,354	—	6,354
	$ 23,775	$ (542)	$ 23,233

Rent expense including executory costs, net of sublease income was $5.4 million for the year ended December 31, 2006, and $3.9 million for both the years ended December 31, 2005 and 2004. One of our directors and officers is Chairman of the Board of Directors and a majority shareholder in AirDefense, Inc. (AirDefense). In August 2006, we assumed from CipherTrust a sublease agreement with AirDefense, subleasing approximately 13,997 square feet of the 75,288 square feet leased office space located in Alpharetta, GA. For the years ending December 31, 2007, 2008, and 2009 we expect to receive $210,000, $210,000 and $122,000, respectively, from AirDefense according to the terms of the sublease agreement. Sublease income is shown on the consolidated results of operation as a reduction of general and administrative expenses.

10. Share-Based Compensation

Description of Plans

2002 Stock Incentive Plan

Under our 2002 Stock Incentive Plan (2002 Plan), we are permitted to grant incentive and non-qualified stock options, restricted stock awards, restricted stock units, stock appreciation rights and other similar types of stock awards, such as phantom stock rights, to our employees and non-employee directors. There were a total of 6.5 million shares authorized under the 2002 Plan at December 31, 2006. All options granted under the 2002 Plan through December 31, 2006 have exercise prices equal to the fair market value of our stock on the date of grant. Options granted under the 2002 Plan have ten-year terms and typically vest 25% after the first year and then monthly over the following three years. All awards granted to non-employee directors vest 100% after the first year. Outstanding awards that were originally granted under several predecessor plans also remain in effect in accordance with their terms. Restricted stock awards vest 25% after the first year, then quarterly thereafter over the following three years, unless otherwise approved by the Compensation Committee.

1995 Omnibus Stock Option Plan

In September 1995, our Board of Directors and stockholders approved our 1995 Omnibus Stock Plan. The majority of options granted under this plan had ten year terms and vested either annually over three years, or fully vested at the end of three years. Beginning in 2003, all new stock options granted under this plan vest 25% after the first year and then monthly over the following three years. This plan expired in September 2005. As of December 31, 2006, there were 5.1 million options outstanding under this Plan, of which 380,283 were not yet vested.

Table of Contents

N2H2 Stock Option Plans

In connection with our acquisition of N2H2 in October 2003, we assumed all of the outstanding N2H2 stock options under the 1997 Stock Option Plan, 1999 Stock Option Plan, 1999 Non-Employee Director Plan, 1999/2000 Transition Plan, the 2000 Stock Option Plan, and the Howard Philip Welt Plan, which were converted into options to purchase approximately 420,000 shares of our common stock. All stock options assumed were exercisable and vested. These options were assumed at prices between $1.55 and $258.63 per share, with a weighted average exercise price of $10.06 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

CyberGuard Stock Option Plans

In connection with our acquisition of CyberGuard in January 2006, we assumed all of the outstanding CyberGuard stock options under the 1994 and 1998 Stock Option Plans which were converted into options to purchase 3,039,545 shares of our common stock. All outstanding stock options assumed were exercisable and vested. These options were assumed at prices between $1.56 and $15.07 per share, with a weighted average exercise price of $7.21 per share. The options granted under these plans, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

CipherTrust 2000 Stock Option Plan

In connection with our acquisition of CipherTrust in August 2006, we assumed all of the outstanding CipherTrust stock options under the 2000 Stock Option Plan which were converted into 2,543,662 shares of our common stock. All outstanding stock options assumed were unvested and have seven-year terms. These options were assumed at prices between $0.01 and $6.19 per share, with a weighted average exercise price of $2.88 per share. The options granted under this plan, since the acquisition, have ten year terms and vest 25% after the first year and then monthly over the following three years.

Employee Stock Purchase Plan

We have an employee stock purchase plan (ESPP), which enables employees to contribute up to 10% of their compensation toward the purchase of our common stock at the end of the participation period at a purchase price equal to 85% of the lower of the fair market value of the common stock on the first or last day of the participation period. For the fourth quarter of 2006 and the first quarter of 2007, the Board of Directors and the Compensation Committee have approved to increase the maximum contribution up to 20% of compensation. Common stock reserved for future employee purchases under the plan totals 589,534 shares at December 31, 2006. Common stock issued under the plan totaled approximately 279,000 in 2006, 164,000 in 2005 and 165,000 in 2004.

Impact of the Adoption of SFAS No. 123(R)

See Note 1 for a description of our adoption of SFAS No. 123(R), on January 1, 2006. A summary of the share-based compensation expense that we recorded in accordance with SFAS No. 123(R) for the twelve months ended December 31, 2006 for stock options, restricted stock and shares purchased under our ESPP is as follows (in thousands, except per share amounts):

	Year Ended December 31, 2006
Cost of product revenues	$ 357
Cost of service revenues	567
Selling and marketing	5,260
Research and development	2,542
General and administrative	1,830
Increase of loss before income taxes	$ 10,556
Increase of basic loss per share	$ (0.19)

Table of Contents

Prior to the adoption of SFAS No. 123(R), we presented all tax benefits for deductions resulting from the exercise of stock options as operating cash flows on our statement of cash flows. SFAS No. 123(R) requires the cash flows resulting from the tax benefits for tax deductions in excess of the compensation expense recorded for those options (excess tax benefits) to be classified as financing cash flows. There were no excess tax benefits for the year ended December 31, 2006.

Determining Fair Value

Valuation and Amortization Method. We estimate the fair value of stock options granted using the Black-Scholes option valuation model. For options granted before January 1, 2006, we amortize the fair value on an accelerated basis. For options granted on or after January 1, 2006, we amortize the fair value on a straight-line basis. All options are amortized over the requisite service periods of the awards, which are generally the vesting periods. For restricted stock, the fair value is calculated as the market price on date of grant and we amortize the fair value on a straight-line basis over the requisite service period of the award, which is generally the vesting period.

Expected Term. The expected term of options granted represents the period of time that they are expected to be outstanding. In light of new accounting guidance under SFAS No. 123(R) and SAB No. 107, we reevaluated our expected term assumption used in estimating the fair value of employee options. We estimate the expected term of options granted based on historical exercise patterns, which we believe are representative of future behavior. Our estimate of the expected life of new options granted to our employees is 3 years, consistent with prior periods. We have examined our historical pattern of option exercises in an effort to determine if there were any discernable patterns of activity based on certain demographic characteristics. Demographic characteristics tested included age, salary level, job level and geographic location. We have determined that there were no meaningful differences in option exercise activity based on the demographic characteristics tested.

Expected Volatility. Also in light of implementing SFAS No. 123(R), we reevaluated our expected volatility assumption used in estimating the fair value of employee options. We estimate the volatility of our common stock at the date of grant based on historical volatility, consistent with SFAS No. 123(R) and SAB No. 107. Our decision to use historical volatility instead of implied volatility was based upon analyzing historical data along with the lack of availability of history of actively traded options on our common stock.

Risk-Free Interest Rate. We base the risk-free interest rate that we use in the Black-Scholes option valuation model on the implied yield in effect at the time of option grant on U.S. Treasury zero-coupon issues with equivalent remaining terms.

Dividends. We have never paid cash dividends on our common stock and we do not anticipate paying cash dividends in the foreseeable future. Consequently, we use an expected dividend yield of zero in the Black-Scholes option valuation model.

Forfeitures. SFAS No. 123(R) requires us to estimate forfeitures at the time of grant and revise those estimates in subsequent periods if actual forfeitures differ from those estimates. We use historical data to estimate pre-vesting option forfeitures and record share-based compensation expense only for those awards that are expected to vest. For purposes of calculating pro forma information under SFAS No. 123 for periods prior to 2006, we accounted for forfeitures as they occurred.

Table of Contents

We used the following assumptions to estimate the fair value of options granted and shares purchased under our ESPP for the twelve months ended December 31, 2006, 2005 and 2004, respectively:

	Year Ended December 31,		
	2006	2005	2004
Stock Options – Assumptions used:			
Average expected terms (years)	3	3	5
Weighted-average volatility	83.0%	85.0%	97.0%
Risk-free interest rate	4.8%	3.9%	3.6%
Dividend yield	0%	0%	0%
ESPP – Assumptions used:			
Average expected terms (years)	0.25	0.25	0.25
Weighted-average volatility	56.5%	48.8%	74.4%
Risk-free interest rate	4.6%	3.2%	1.4%
Dividend yield	0%	0%	0%

The Black-Scholes option-pricing model was developed for use in estimating the fair value of traded options that have no vesting restrictions and are fully transferable. In addition, option valuation models require the input of highly subjective assumptions, including the expected stock price volatility. Because changes in the subjective input assumptions can materially affect the fair value estimate, in our opinion, the existing models do not necessarily provide a reliable single value of our options and may not be representative of the future effects on reported net income or loss or the future stock price of our company.

Share-Based Compensation Expense and Stock Option Activity

For the year ended December 31, 2006, we recorded $10.6 million in share-based compensation expense, which includes $9.4 million for stock options, $529,000 for our ESPP and $637,000 for restricted stock. At December 31, 2006, we had 373,000 non-vested restricted stock awards that had a weighted average grant date fair value of $9.80. As of December 31, 2006, there was $32.7 million of total unrecognized compensation cost related to non-vested share-based compensation arrangements granted under all equity compensation plans. Total unrecognized compensation cost will be adjusted for future changes in estimated forfeitures. We expect to recognize that cost over a weighted average period of 3.1 years.

A summary of stock option activity under all stock plans during the year ended December 31, 2006 is as follows:

	Stock Options	Weighted Average Exercise Price per Share	Weighted Average Remaining Contractual Life (Years)	Aggregate Intrinsic Value
Outstanding at December 31, 2005	8,549,315	$ 10.06	6.5	$18,793,738
Granted	4,614,199	8.28	9.8	—
Assumed upon acquisition of CyberGuard	3,039,545	7.21	3.5	—
Assumed upon acquisition of CipherTrust	2,543,662	2.88	2.6	—
Exercised	(1,418,544)	4.51	—	7,934,248
Cancelled/forfeited/expired	(1,467,625)	8.58	—	—
Outstanding at December 31, 2006	15,860,552	8.52	6.6	11,608,819
Shares vested and expected to vest	15,064,588	8.97	6.8	11,585,629
Exercisable at December 31, 2006	8,637,863	$ 9.45	5.2	$ 6,172,481

We define in-the-money options at December 31, 2006 as options that had exercise prices that were lower than the $6.56 market price of our common stock at that date. The aggregate intrinsic value of options outstanding at December 31, 2006 is calculated as the difference between the exercise price of the underlying options and the market price of our common stock for the 4.0 million shares that were in-the-money at that date. There were 2.1 million in-the-money options exercisable at December 31, 2006. During the year ended December 31, 2006, 373,000 shares of restricted stock were awarded to employees and directors, of which none had vested as of December 31, 2006. There were no restricted stock awards prior to 2006.

We received $6.4 million in cash from option exercises under all share-based payment arrangements for the year ended December 31, 2006.

Comparable Disclosure

Prior to January 1, 2006, we accounted for our share-based compensation plans under the recognition and measurement provisions of APB Opinion No. 25 and related Interpretations. No share-based employee compensation cost is reflected in the condensed consolidated statements of operations for the years ended December 31, 2005 and 2004, as all options granted under those plans had an exercise price equal to the market value of the underlying common stock on the date of grant. The following table illustrates the effect on net income and net income per share if we had applied the fair value recognition provisions of SFAS No. 123 to share-based employee compensation prior to January 1, 2006 (in thousands, except per share amounts):

	Year Ended December 31,	
	2005	2004
Net income, as reported	$ 21,374	$ 12,835
Deduct: Total stock-based employee compensation expense determined under fair value based method for all awards, net of related tax effects	(10,454)	(11,728)
Pro forma net income	$ 10,920	$ 1,107
Net income per share:		
Basic – as reported	$ 0.59	$ 0.36
Basic – pro forma	$ 0.30	$ 0.03
Diluted – as reported	$ 0.57	$ 0.34
Diluted – pro forma	$ 0.29	$ 0.03

11. Defined Contribution Plans

We have a voluntary defined contribution plan under Section 401(k) of the Internal Revenue Code that covers substantially all U.S. employees. Through 2006 the 401(k) plan provided a discretionary year-end employer matching contribution on employee deferral contributions made during the plan year. The employer matching contribution will be made quarterly in 2007. Employer contributions made to the 401(k) plan were $401,000 during 2006, $274,000 during 2005, and none during 2004.

12. Income Taxes

For financial reporting purposes, (loss) income before income taxes includes the following components (in thousands):

	Year Ended December 31,		
	2006	2005	2004
(Loss) income before income taxes:			
U.S.	$(19,747)	$21,425	$12,352
Non U.S. subsidiaries	1,854	557	483
Total (loss) income before income taxes	$(17,893)	$21,982	$12,835

During 2006, we recorded income tax expense of $9.5 million. Of this $9.5 million income tax expense, a non-cash expense of $8.5 million is related to a net tax valuation allowance recorded on our net deferred tax

assets. We were unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses, and needed to provide tax expense for the subsequent valuation allowance reapplied to the remaining net operating losses. This was a result of changes in circumstances due to recent acquisitions that caused a change in judgment regarding the realizability of our net deferred tax assets in the fourth quarter. The remainder of the income tax expense is related to current income tax components such as, alternative minimum income tax, and state and foreign income taxes. This is compared with $608,000 of income tax expense recorded in 2005 which consisted of $349,000 for alternative minimum tax expense, $58,000 for state income tax expense and $201,000 for various foreign income tax expenses.

Federal alternative minimum tax was provided on the portion of our alternative minimum taxable income which could not be entirely offset by the alternative tax net operating loss deduction carryforward which we have available. Similar to 2006, we anticipate that we will be in an alternative minimum taxable income position in 2007. Current tax law provides that part or all of the amount of the alternative minimum tax paid can be carried forward indefinitely and credited against federal regular tax in future tax years to the extent the regular tax liability exceeds the alternative minimum tax in those years. For 2006, the reversal of $3.1 million of the tax valuation allowance related to acquired net operating losses was recorded as a decrease to goodwill in the balance sheet and not as a benefit to tax expense in the income statement.

The components for the provision for income taxes were as follows (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Current income tax expense:			
U.S.	$ 465	$349	$ —
States (U.S.)	212	58	62
Non U.S. subsidiaries	644	201	283
Deferred income tax expense:			
U.S.	7,459	—	(345)
States (U.S.)	725	—	—
Non U.S. subsidiaries	—	—	—
Total income tax expense	$9,505	$608	$ —

A reconciliation of our provision for income taxes to the statutory tax rate based upon pretax (loss) income was as follows (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Income taxes at U.S. statutory tax rate	$ (6,262)	$ 7,739	$ 4,264
State taxes, net of federal benefit	(137)	734	249
Non U.S. tax rate differential	(310)	6	203
Change in valuation allowance	12,870	(10,543)	(4,663)
Change in deferred tax rate	—	3,066	—
Change in tax credit carryforwards	—	(360)	—
Stock-based compensation	2,257	—	—
Imputed income	623	—	—
Other	464	(34)	(53)
Total income tax expense	$ 9,505	$ 608	$ —

Table of Contents

Deferred income tax assets and liabilities result from temporary differences between the carrying values of assets and liabilities for financial statement and income tax purposes. Significant components of our net deferred tax assets and liabilities are as follows (in thousands):

	As of December 31,		
	2006	2005	2004
Deferred tax assets:			
Accrued liabilities	$ 1,104	$ 538	$ 1,086
Payroll liabilities	638	363	239
Tax assets over book assets	3,956	—	—
Tax over book amortization	1,861	(864)	(612)
Book over tax depreciation	—	619	93
Deferred revenue	4,164	2,034	—
Stock compensation	1,188	—	—
Income tax credits	1,095	838	478
Net operating loss carryforward	110,603	68,236	79,172
Total deferred tax assets before valuation allowance	124,609	71,764	80,456
Less valuation allowance	(100,225)	(68,160)	(76,852)
Net deferred tax assets after valuation allowance	24,384	3,604	3,604
Deferred tax liabilities:			
Acquired indefinite lived intangibles	7,672	—	—
Acquired definite lived intangibles	22,724	—	—
Other deferred tax liabilities	1,660	—	—
Total deferred tax liabilities	32,056	—	—
Net deferred tax (liabilities) assets	$ (7,672)	$ 3,604	$ 3,604

In accordance with SFAS No. 109, we have assessed the likelihood that the net deferred tax assets will be realized. SFAS No. 109, "Accounting for Income Taxes," requires the consideration of a valuation allowance in all circumstances, if the conclusion is not more likely than not a valuation allowance is required. We have determined that it is more likely than not that deferred tax assets of $24.4 million at December 31, 2006 will be realized based on our expected future reversals of certain deferred tax liabilities. We have a net deferred tax liability recorded in our balance sheet that consists primarily of indefinite lived intangible assets that are not deductible for tax purposes and therefore cannot be used to realize additional reversing deferred tax assets. In accordance with SFAS No. 109, our remaining noncurrent deferred tax liabilities are netted with our noncurrent deferred tax assets and are presented as a single amount in our consolidated balance sheet.

Worldwide net operating loss carryforwards totaled approximately $479.5 million at December 31, 2006, comprised of $456.6 million domestic net operating loss carryforwards and $22.9 million of international net operating loss carryforwards. These carryforwards are available to offset taxable income through 2026 and will start to expire in 2011. Of these carryforwards, $208.1 million relates to acquired CyberGuard net operating losses, $59.6 million relates to acquired N2H2 net operating losses, and $19.4 million relates to acquired CipherTrust net operating losses. We have provided a complete valuation allowance on primarily all of these acquired losses are fully valued against, and upon release of the valuation allowance, a portion of the benefit will go to the balance sheet to reduce goodwill instead of a benefit to the income tax provision. As of December 31, 2006 we have deducted $56.8 million related to stock option exercises. The tax benefit in excess of book expense from these stock option exercises will be recorded as an increase to additional paid-in capital upon utilization of the net operating losses under the financial statement approach to recognizing the tax benefits associated with stock option deductions. Of the remaining benefit associated with the carryforwards, approximately $111.3 million has yet to be recognized in the consolidated statement of operations. However, there are no assurances that the tax benefit of these carryforwards will be available to offset future income tax expense when taxable income is realized.

Table of Contents

No provision has been made for U.S. federal income taxes on certain cumulative undistributed earnings of non U.S. subsidiaries as we intend to indefinitely reinvest these earnings in the non U.S. subsidiaries or the earnings may be remitted substantially tax-free. The total cumulative undistributed earnings of certain of our non U.S. subsidiaries that would be subject to federal income tax if remitted under existing law is approximately $5.9 million at December 31, 2006. Determination of the unrecognized deferred tax liability related to these earnings is not practicable because of the complexities with its hypothetical calculation. Upon distribution of these earnings, we may be subject to U.S. taxes and withholding taxes payable to various foreign governments.

13. Contingencies

In December 2002, we were named as the defendant in a rental property lawsuit brought by Salvio Pacheco Square LLP in the Superior Court of California, County of Contra Costa. The complaint alleges that we breached a commercial lease at our Concord, CA office and asked for declaratory relief, and compensatory and other damages. The Superior Court entered judgment in favor of plaintiff in June 2004 in the amount of $1.1 million and found we had breached the lease. We appealed to the First Appellate District, California Court of Appeal. The Court of Appeal denied our appeal in April 2006. In addition to the judgment entered by the Superior Court in June 2004, we incurred additional costs of $1.4 million as damages for the rental and other costs due on the balance of the lease, interest on the judgment and unpaid amounts due under the lease and plaintiff's attorney's fees and costs. As a result of the April 2006 denial of our appeal, we accrued $2.5 million as of March 31, 2006 for the settlement of this litigation. The settlement of $2.5 million was subsequently paid in July 2006.

On June 5, 2006, Finjan Software, Ltd. filed a complaint entitled Finjan Software, Ltd. v. Secure Computing Corporation in the United States District Court for the District of Delaware against Secure Computing Corporation, CyberGuard Corporation, and Webwasher AG. The complaint alleges that Secure Computing and its named subsidiaries infringe U.S. Patent No. 6,092,194 ("'194 Patent") based on the manufacture, use, and sale of the Webwasher Secure Content Management suite. Secure Computing denies infringing any valid claims of the '194 Patent. The answer to the complaint was filed on July 26, 2006. Discovery is proceeding.

On January 19, 2007, Rosenbaum Capital, LLC filed a putative securities class action complaint in the United States District Court for the Northern District of California against us and certain directors and officers of the company. The alleged plaintiff class includes persons who acquired stock between May 4, 2006 through July 11, 2006. The complaint alleges generally that defendants made false and misleading statements about our business condition and prospects for the fiscal quarter ended June 30, 2006, in violation of Section 10(b) and 20(a) of the Securities Exchange Act of 1934 and SEC Rule 10b-5. The complaint seeks unspecified monetary damages. While there can be no assurance as to the outcome of this or any other litigation we believe there are meritorious legal and factual defenses to this action and we intend to defend ourselves vigorously.

From time to time we may be engaged in certain other legal proceedings and claims arising in the ordinary course of our business. The ultimate liabilities, if any, which may result from these or other pending or threatened legal actions against us cannot be determined at this time. However, in the opinion of management, the facts known at the present time do not indicate that such litigation will have a material effect on our consolidated financial position or results of operation.

Table of Contents

14. Net (Loss)/Income Per Share

The following table represents the calculation of basic and diluted net (loss)/income per share (in thousands, except per share amounts):

	Year Ended December 31,		
	2006	2005	2004
Net (loss)/income applicable to common stockholders	$(43,551)	$21,374	$12,835
Shares used in computing basic net (loss)/income per share	57,010	36,338	35,576
Outstanding dilutive stock options	—	1,371	1,680
Shares used in computing diluted net (loss)/income per share	57,010	37,709	37,256
Basic net (loss)/income per share	$ (0.76)	$ 0.59	$ 0.36
Diluted net (loss)/income per share	$ (0.76)	$ 0.57	$ 0.34

All potential common share equivalents for the year ended December 31, 2006 were excluded from the computation of diluted earnings per share as inclusion of these shares would have been anti-dilutive. Additionally, 5.6 million shares of common stock as if our preferred stock was converted, were excluded from the effect of dilutive securities for the year ended December 31, 2006, because we reported a net loss for this period. Potential common shares of 2.6 million and 2.5 million related to our outstanding stock options were excluded from the computation of diluted earnings per share for 2005 and 2004, respectively, as inclusion of these shares would have been anti-dilutive.

15. Segment Information

We view our operations and manage our business as one segment called enterprise gateway security. Major foreign markets for our products and services include Europe, Japan, China, the Pacific Rim, and Latin America. In each market, we have independent channel partners who are responsible for marketing, selling and supporting our products and services to resellers and end-users within their defined territories. International sales accounted for 39%, 38% and 31% of total revenue for the years 2006, 2005 and 2004, respectively.

The following table summarizes our domestic and international revenues (in thousands):

	Year Ended December 31,		
	2006	2005	2004
Revenues:			
Domestic	$108,547	$ 67,689	$64,431
International	68,150	41,486	28,947
	$176,697	$109,175	$93,378

No customer accounted for more than 10% of our total revenue in 2006, 2005 or 2004.

16. Related Party Transaction

In February 2005, we made a strategic investment in a privately-held technology company. As a result of this $2.7 million investment, we have a 15% ownership stake in this company. This investment is reported in other assets on our consolidated balance sheets and is evaluated for impairment annually.

Two of our board members, one of whom is a board member of the investee, are individual investors of the investee. Due to their involvement with the investee, these two board members recused themselves from our decision to make the investment.

Table of Contents

17. Summarized Quarterly Financial Information (unaudited)

	Quarter Ended (in thousands, except per share data)			
	March 31,	June 30,	September 30,	December 31,
2006				
Revenue	$ 42,617	$38,746	$ 43,748	$ 51,586
Gross profit	30,685	28,822	31,963	36,069
Operating income/(loss) (1)	769	(2,710)	(6,347)	(9,485)
Net income/(loss) (2)	657	6,659	(7,291)	(27,423)
Net (loss)/income applicable to common shareholders	(12,759)	5,722	(8,194)	(28,320)
Basic and diluted (loss)/income per share	$ (0.25)	$ 0.11	$ (0.14)	$ (0.44)
2005				
Revenue	$ 25,579	$26,113	$ 27,249	$ 30,234
Gross profit	20,594	21,578	22,217	22,737
Operating income	4,121	4,746	5,404	6,080
Net income	4,062	4,946	5,792	6,574
Basic income per share	$ 0.11	$ 0.14	$ 0.16	$ 0.18
Diluted income per share	$ 0.11	$ 0.13	$ 0.15	$ 0.17

(1) Operating loss for the quarter ended June 30, 2006 was negatively impacted by the reduction in revenue recognized in that quarter. For the quarters ended September 30, 2006 and December 31, 2006, operating loss was impacted by the acquisition of CipherTrust. Because we are unable to establish VSOE of fair value on the CipherTrust product line revenues, the majority of the revenue from those product lines has been deferred, while the operating expenses continue to be recognized in the current periods, resulting in a net operating loss impact.

(2) Net income for the quarter ended June 30, 2006 included the impact of benefiting from the reversal of $7.3 million of valuation allowance that had been established against our deferred tax assets. Net loss for the quarter ended December 31, 2006 included a net $15.5 million tax expense due to being unable to benefit from the initial release of valuation allowance on utilized acquired net operating losses and an increase in the valuation allowance established against our deferred tax assets.

Table of Contents

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of Secure Computing Corporation

We have audited the accompanying consolidated balance sheets of Secure Computing Corporation as of December 31, 2006 and 2005, and the related consolidated statements of operations, stockholders' equity, and cash flows for each of the three years in the period ended December 31, 2006. Our audits also included the financial statement schedule listed in the Index at Item 15(a). These consolidated financial statements and schedule are the responsibility of the Company's management. Our responsibility is to express an opinion on these financial statements and schedule based on our audits.

We conducted our audits in accordance with the standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audits provide a reasonable basis for our opinion.

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the consolidated financial position of Secure Computing Corporation at December 31, 2006 and 2005, and the consolidated results of its operations and its cash flows for each of the three years in the period ended December 31, 2006, in conformity with U.S. generally accepted accounting principles. Also, in our opinion, the related financial statement schedule, when considered in relation to the basic consolidated financial statements taken as a whole, presents fairly in all material respects the information set forth therein.

As discussed in Note 1, Summary of Significant Accounting Policies, to the consolidated financial statements, effective January 1, 2006, the Company adopted Statement of Financial Accounting Standards No. 123 (revised 2004), Share-Based Payment, using the modified prospective method.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States), the effectiveness of Secure Computing Corporation's internal control over financial reporting as of December 31, 2006, based on criteria established in *Internal Control—Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission, and our report dated March 15, 2007, expressed an unqualified opinion on management's assessment and an adverse opinion on the effectiveness of internal control over financial reporting.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007

Table of Contents

Report of Independent Registered Public Accounting Firm

The Board of Directors and Stockholders of Secure Computing Corporation

We have audited management's assessment, included in the section in Item 9A entitled Management's Report on Internal Control Over Financial Reporting, that Secure Computing Corporation did not maintain effective internal control over financial reporting as of December 31, 2006, because of the effect of ineffective controls over the calculation of income taxes, based on criteria established in *Internal Control—Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (the COSO criteria). Secure Computing Corporation's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting. Our responsibility is to express an opinion on management's assessment and an opinion on the effectiveness of the company's internal control over financial reporting based on our audit.

We conducted our audit in accordance with standards of the Public Company Accounting Oversight Board (United States). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, evaluating management's assessment, testing and evaluating the design and operating effectiveness of internal control, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies and procedures may deteriorate.

A material weakness is a control deficiency, or combination of control deficiencies, that results in more than a remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. A material weakness has been identified and described in management's assessment related to an ineffective control over the accounting for income taxes as evidenced by a failure to detect necessary adjustments to the income tax accounts. This deficiency resulted in material adjustments being made to the annual financial statements and rises to the level of a material weakness. This material weakness was considered in determining the nature, timing, and extent of audit tests applied in our audit of the 2006 financial statements, and this report does not affect our report dated March 15, 2007 on those financial statements.

As indicated in the accompanying Management's Report on Internal Control Over Financial Reporting, management's assessment of and conclusion on the effectiveness of internal control over financial reporting did not include the internal controls of the business operations of CipherTrust, Inc. which are included in the 2006 consolidated financial statements of Secure Computing Corporation and constituted approximately $66.0 million and $19.1 million of total and net assets, respectively, as of December 31, 2006 and $7.1 million of revenues for

Table of Contents

the year then ended. Our audit of internal control over financial reporting of Secure Computing Corporation also did not include an evaluation of the internal control over financial reporting of the business operations of CipherTrust, Inc.

In our opinion, management's assessment that Secure Computing Corporation did not maintain effective internal control over financial reporting as of December 31, 2006, is fairly stated, in all material respects, based on the COSO criteria. Also, in our opinion, because of the material weakness described above on the achievement of objectives of the control criteria, Secure Computing Corporation has not maintained effective internal control over financial reporting as of December 31, 2006, based on the COSO criteria.

/s/ Ernst & Young LLP

Minneapolis, Minnesota
March 15, 2007

Table of Contents

SECURE COMPUTING CORPORATION

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, as amended, the Registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

SECURE COMPUTING CORPORATION

Date: March 16, 2007

By: /s/ JOHN E. MCNULTY
John E. McNulty
Chairman, President and Chief Executive Officer

Table of Contents

Power of Attorney

KNOW ALL MEN BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints John McNulty and Timothy Steinkopf or either of them, his or her true and lawful attorneys-in-fact and agents, with full power of substitution and re-substitution, for him or her and in his or her name, place and stead, in any and all capacities to sign any and all amendments to this Report on Form 10-K, and to file the same, with all exhibits thereto and other documents in connection therewith, with the Securities and Exchange Commission, granting unto the attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that the attorneys-in-fact and agents, or either of them, or their, his or her substitutes or substitute, may lawfully do or cause to be done by virtue hereof.

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed by the following persons on behalf of the Registrant and in the capacities indicated on March 16, 2007.

Signature	Title
/s/ JOHN E. MCNULTY John E. McNulty	Chairman, President and Chief Executive Officer (Principal Executive Officer)
/s/ TIMOTHY J. STEINKOPF Timothy J. Steinkopf	Senior Vice President of Operations and Chief Financial Officer (Principal Financial and Accounting Officer)
/s/ JAY S. CHAUDHRY Jay S. Chaudhry	Vice Chairman and Chief Strategy Officer
/s/ ROBERT J. FRANKENBERG Robert J. Frankenberg	Director
/s/ JAMES F. JORDAN James F. Jordan	Director
/s/ STEPHEN M. PURICELLI Stephen M. Puricelli	Director
/s/ ERIC P. RUNDQUIST Eric P. Rundquist	Director
/s/ ALEXANDER ZAKUPOWSKY, JR. Alexander Zakupowsky, Jr.	Director
/s/ CARY DAVIS Cary Davis	Director
/s/ RICHARD SCOTT Richard Scott	Director

Table of Contents

SCHEDULE II
VALUATION AND QUALIFYING ACCOUNTS
YEARS ENDED DECEMBER 31, 2006, 2005 AND 2004

Description	Balance at Beginning of Year	Additions Charged to Bad Debt Expense	Adjustments to Goodwill	Deductions-Write-offs	Balance at End of Year
Year ended December 31, 2006:					
Allowance for doubtful accounts (1)	$272,000	$947,000	$ 802,000	$(594,000)	$1,427,000
Year ended December 31, 2005:					
Allowance for doubtful accounts	$450,000	$ 69,000	$ —	$(247,000)	$ 272,000
Year ended December 31, 2004:					
Allowance for doubtful accounts (2)	$868,000	$212,000	$(320,000)	$(310,000)	$ 450,000

(1) The amount noted as an adjustment to goodwill reflects the balance of acquired CipherTrust receivables outstanding that are fully reserved as of December 31, 2006.

(2) The amount noted as an adjustment to goodwill reflects the finalization of the purchased N2H2 receivables and therefore, did not impact earnings.

EXHIBIT 27

IDC

MARKET ANALYSIS

Worldwide Secure Content and Threat Management 2007–2011 Forecast and 2006 Vendor Shares: 1 + 1 = 4

Brian E. Burke
Jon Crotty
Charles J. Kolodgy

IDC OPINION

Secure content management (SCM) technologies have converged with threat management (TM) technologies across all layers of network security. In light of this convergence, IDC has combined the SCM and TM markets and created four new submarkets: network security, endpoint security, messaging security, and Web security. Key trends in the convergence of SCM and TM include:

- IT departments have moved away from a focus on a single type of protection, such as antivirus, toward a broader focus on today's complex threats designed to get past point-solution security and target multiple vulnerabilities in clients and corporate networks. Unified threat management (UTM) appliances are an example of the convergence of network SCM (antivirus, Web filtering) with network TM (firewall/VPN, intrusion prevention) to provide a comprehensive security solution addressing today's complex threat environment.

- In the past, organizations commonly implemented best-of-breed antivirus, antispam, firewall, and intrusion detection technologies. As security technologies became more complex, managing a variety of point products became significantly more difficult. Secure content and threat management (SCTM) solutions help reduce the complexity of installation and configuration while at the same time providing an integrated response capability across a variety of security technologies.

- Customers are demanding integration between individual security technologies to reduce the cost and time associated with managing point products. Integrated SCTM solutions are playing a key role in reducing administrative and support costs and, ultimately, reducing the total cost of ownership (TCO) of managing multiple security technologies.

- Attackers have moved from hobbyists to professionals. This greatly increases the complexity of threats, thus making it much more difficult for a single SCM or TM technology to detect and prevent the attack.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

Filing Information: June 2007, IDC #207523, Volume: 1, Tab: Markets

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

IN THIS STUDY

This study examines the SCTM market for the period from 2005 to 2011, with vendor revenue trends and market growth forecasts. Worldwide market sizing is provided for 2006, with trends from 2005. A five-year growth forecast for this market is shown for 2007–2011. The revenue and market share of the leading vendors are provided for 2006.

Methodology

See the Learn More section for a description of the forecasting and analysis methodology employed in this study.

In addition, please note the following:

- The information contained in this study was derived from the IDC Software Market Forecaster database as of June 18, 2007.
- All numbers in this document may not be exact due to rounding.
- For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2007* (IDC #205437, February 2007).

Secure Content and Threat Management Market Definition

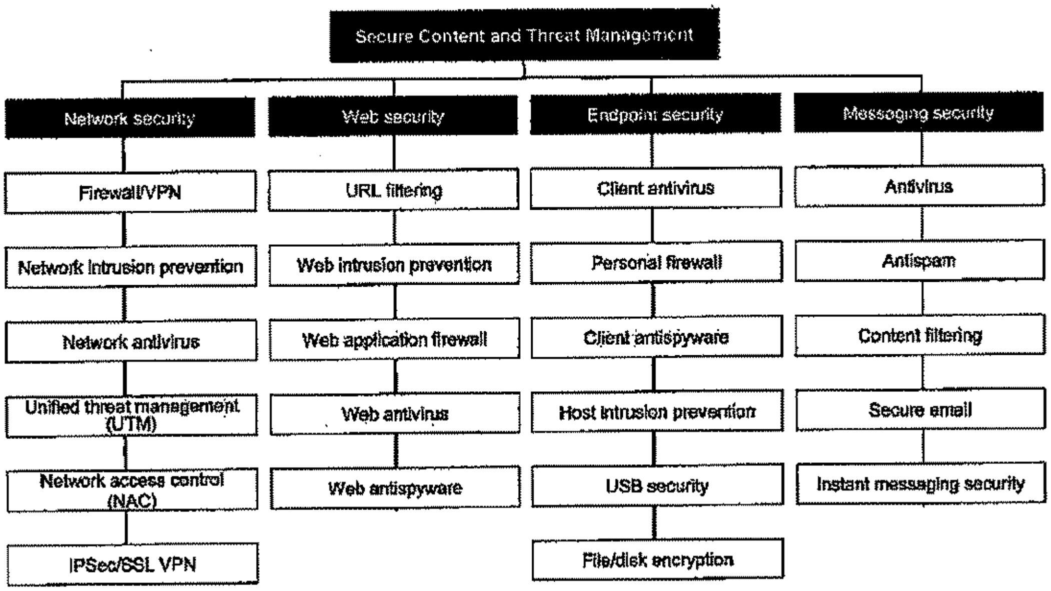
The secure content and threat management (SCTM) market highlights the increasing unity between previously dissimilar security disciplines. SCTM products defend against viruses, spyware, spam, hackers, intrusions, and the unauthorized use or disclosure of confidential information. Products in this market are offered as standalone software, software married to dedicated appliances, and hosted software services. Revenue from all of these product offerings are tracked under software to provide a holistic representation of the SCTM product market. SCTM includes four specific product areas, as follows and as shown in Figure 1:

- **Network security** includes enterprise firewall/VPN products, network intrusion detection and prevention products, network antivirus products, unified threat management products, IPSec/SSL VPN products, and network access control products.
- **Endpoint security** includes client antivirus products, file/storage server antivirus, client antispyware products, desktop firewall products, host intrusion prevention products, file/disk encryption, and endpoint information protection and control products (IPC).
- **Messaging security** includes antispam products, mail server antivirus, content filtering, email encryption, and messaging information protection and control products.

- **Web security** includes Web filtering products, Web application firewall products, Web intrusion prevention products, Web antivirus products, Web antispyware products, and Web content filtering products.

FIGURE 1

Convergence of Secure Content and Threat Management



Source: IDC, 2007

SITUATION OVERVIEW

Mergers and Acquisitions Highlight Convergence of Secure Content and Threat Management

There have been several mergers and acquisitions over the past 18 months that highlight the convergence of secure content management with threat management:

- On January 4, 2007, **Cisco** announced that it intends to acquire privately held **IronPort** for approximately US$830 million in cash and stock. This acquisition is a perfect example of the convergence of SCM and TM. Cisco will extend its self-defending network strategy, which is currently based on a security portfolio that includes classic network security technologies (e.g., firewalls, intrusion prevention systems, and VPNs) and network-oriented endpoint security technologies (e.g., NAC and personal firewall) in a variety of form factors.

IronPort's secure content management appliances and technology will broaden the portfolio and provide a rich and complementary suite of messaging solutions to Cisco's threat mitigation, confidential communications, policy control, and management solutions. The IronPort acquisition will also allow Cisco to go to market with a more convincing and complete service oriented network architecture (SONA) framework, which outlines how enterprises can evolve their IT infrastructure to have a greater impact on business.

- On July 11, 2006, **Secure Computing Corp.** announced that it has signed a definitive agreement to acquire **CipherTrust Inc.**, a global leader in messaging security. CipherTrust, a privately held company, provides innovative layered security solutions to stop inbound messaging threats such as spam, viruses, intrusions, and phishing and protects against outbound policy and compliance violations associated with sensitive data leakage. The combined company will be positioned as a leader in the enterprise gateway appliances market, featuring a comprehensive, integrated, and unified portfolio of solutions — including UTM, messaging security, Web filtering, and identity management — with centralized policy and management capabilities. Together, these products will address network gateway and application gateway security for all of the major Internet protocols, including Web (HTTP and FTP), email (SMTP and POP), and instant messaging and identity-based access protection.

- On February 8, 2006, **SonicWALL Inc.** (NASDAQ: SNWL) announced that it has acquired email security company **MailFrontier Inc.** for a consideration of approximately $31 million in an all-cash transaction. The purchase of MailFrontier enables SonicWALL to bring email security to channel partners and their end users as part of its end-to-end suite of secure content protection. MailFrontier's customers will benefit from the integration of SonicWALL's market-leading SCM and UTM capabilities, while SonicWALL's distributed enterprise customers will have access to a further range of offerings for the midmarket.

- On April 26, 2007, **Websense** announced plans to acquire **SurfControl**, one of its longtime competitors in the Web filtering market. IDC believes that Websense acquired SurfControl because it wants to expand beyond Web security into the logically aligned messaging security market. This is a strategic expansion of Websense's market reach. Websense recognizes that customers increasingly want solutions that combine Web security, messaging security, and information protection and control (IPC) (data-leakage protection). This is especially true for small and midtier customers. These same customers are also looking for the flexibility of management services to reduce capital budgets, make operational budgets predictable, and control the need for IT expertise.

- On August 23, 2006, **IBM** (NYSE: IBM) and **Internet Security Systems Inc.** (NASDAQ: ISSX) announced that the two companies have entered into a definitive agreement for IBM to acquire Internet Security Systems Inc., a publicly held company based in Atlanta, Georgia, in an all-cash transaction at a price of approximately $1.3 billion, or $28 per share. ISS, with its RealSecure and Proventia product lines, is a leading vendor in the intrusion detection and prevention markets. According to IDC's Security Appliance Tracker, ISS was the leader in revenue for intrusion prevention appliances in 2005. ISS is also the leader in the network vulnerability assessment market, with its Internet Scanner solution. For IDC, the bottom line on this deal is that in the short term it might depress some ISS revenue, but in the long term it will solidify the growing need to integrate security with overall IT infrastructures. IBM has an opportunity to offer strong security to enterprises as part of its overall management software and managed service offerings.

☒ On January 29, 2007, **Symantec** announced it has signed a definitive agreement to acquire **Altiris Inc.** (Nasdaq: ATRS). Symantec is positioning the Altiris products as part of an overall endpoint security and management portfolio. With the Altiris solutions, Symantec expects to be able to help customers better manage and enforce security policies at the endpoint, identify and protect against threats, and repair and service assets. On January 3, 2006, **Symantec** announced it has signed a definitive agreement to acquire **IMlogic**, a provider of enterprise software for managing and securing instant messaging. From a security standpoint, the explosive growth of IM as a business communications tool has created a host of security threats. IM networks have quickly become an attractive target for the hacker community to distribute virus and worm attacks, Trojan horses, spyware, spam, and other types of malicious code.

☒ On October 15, 2006, **McAfee** (NYSE: MFE) announced an agreement to acquire start-up company **Onigma** for an estimated $20 million. Israeli-based Onigma operates in the field of information protection and control (IPC), an umbrella term for different types of solutions for mitigating the risks of data loss, either through network channels or corporate desktops.

☒ On November 20, 2006, **Check Point Software** (NASDAQ: CHKP), a worldwide leader in threat management, announced a cash tender offer to acquire Protect Data AB (publ) (PROT.ST), the 100% owner of **Pointsec Mobile Technologies**, a global leader for enterprise data security, for approximately US $586 million. PointSec Mobile Technologies is a leading provider of encryption and other security products for PCs, PDAs, and smartphones. Check Point plans to plug this technology into its existing security architecture to offer its clients improved endpoint security technology.

The Secure Content and Threat Management Market in 2006

Performance of Leading Vendors in 2006

Table 1 displays 2004–2006 worldwide revenue and 2006 growth and market share for SCTM vendors. Worldwide revenue for SCTM vendors reached $13.2 billion in 2006, representing growth of 14% over 2005. The top 5 SCTM vendors in 2006 showed the following results:

☒ Symantec led the SCTM market in 2006, with $2.4 billion in revenue and an 18% share of the worldwide market.

☒ Cisco generated $1.6 billion in SCTM revenue in 2006 and accounted for a 12% share of the worldwide market.

☒ McAfee generated $1.1 billion in SCTM revenue in 2006 and accounted for an 8% share of the worldwide market.

☒ Trend Micro generated $727 million in SCTM revenue in 2006 and accounted for a 6% share of the worldwide market.

☒ Check Point generated $501 million in SCTM revenue in 2006 and accounted for a 4% share of the worldwide market.

TABLE 1

Worldwide Secure Content and Threat Management Revenue by Vendor, 2005–2006 ($M)

	2005	2006	2006 Share (%)	2005–2006 Growth (%)
Symantec	2,321.8	2,380.8	18.0	2.5
Cisco	1,462.3	1,587.4	12.0	8.6
McAfee	917.5	1,064.9	8.0	16.1
Trend Micro	621.9	726.8	5.5	16.9
Check Point	531.5	501.0	3.8	-5.7
Juniper Networks	399.4	479.8	3.6	20.1
Microsoft	233.6	280.3	2.1	20.0
Nokia Corp.	225.0	249.1	1.9	10.7
IBM	208.0	230.0	1.7	10.6
Secure Computing Corp.	189.2	196.6	1.5	3.9
Sophos	164.5	195.3	1.5	18.7
Websense	148.6	178.8	1.4	20.3
SonicWALL	127.1	164.3	1.2	29.3
Fortinet	109.0	142.0	1.1	30.3
Panda Software	130.0	131.4	1.0	1.0
SurfControl Inc.	99.9	110.9	0.8	11.0
F-Secure Corp.	74.9	102.4	0.8	36.8
MessageLabs	75.7	96.1	0.7	26.9

TABLE 1

Worldwide Secure Content and Threat Management Revenue by Vendor, 2005–2006 ($M)

	2005	2006	2006 Share (%)	2005–2006 Growth (%)
Webroot	70.0	84.6	0.6	20.8
IronPort Systems	44.0	80.0	0.6	81.8
CA	88.7	78.0	0.6	-12.1
WatchGuard	62.7	71.8	0.5	14.6
Clearswift Corp.	57.1	68.0	0.5	19.0
Kaspersky Lab	39.9	67.0	0.5	67.9
Postini	45.6	60.8	0.5	33.2
Pointsec	25.0	52.0	0.4	108.0
Barracuda Networks Inc.	35.0	52.0	0.4	48.5
PGP Corporation	35.0	50.0	0.4	42.9
Tumbleweed Communication Inc.	41.9	47.2	0.4	12.8
ESET	19.8	43.7	0.3	120.5
Ahnlab Inc.	36.6	43.0	0.3	17.6
Sourcefire	30.9	41.9	0.3	35.6
Grisoft	29.0	37.6	0.3	29.6
Norman ASA	30.6	35.1	0.3	14.8
SafeNet Inc.	13.8	32.6	0.2	135.7
Workshare	20.0	32.1	0.2	60.5
Aventail	26.0	29.0	0.2	11.7
Vontu	13.6	28.8	0.2	111.4
Novell	25.8	27.4	0.2	6.0
Citrix	15.0	25.9	0.2	72.7
Astaro	16.9	25.8	0.2	52.9
Entrust Inc.	26.2	23.8	0.2	-9.3

TABLE 1

Worldwide Secure Content and Threat Management Revenue by Vendor, 2005–2006 ($M)

	2005	2006	2006 Share (%)	2005–2006 Growth (%)
Enterasys Networks Inc.	19.0	21.9	0.2	15.1
Utimaco Safeware AG	12.0	21.4	0.2	78.2
Borderware	14.0	20.0	0.2	42.9
ZixCorp	16.3	19.8	0.1	21.8
Finjan Software Ltd.	16.4	19.7	0.1	19.8
Sun Microsystems	16.9	19.5	0.1	15.2
Credant Technologies	12.5	17.0	0.1	36.0
Proofpoint Inc.	12.0	16.8	0.1	40.0
Mirapoint	15.4	15.7	0.1	1.9
St. Bernard Software	12.0	14.5	0.1	20.7
8e6 Technologies	11.5	13.8	0.1	20.3
Hauri Inc.	11.0	13.0	0.1	17.7
Aladdin Knowledge Systems	11.2	12.3	0.1	9.8
MX Logic	8.6	12.0	0.1	39.5
StoneSoft Corp.	11.9	12.0	0.1	0.8
Tripwire Inc.	10.0	11.4	0.1	14.0
FaceTime Communications Inc.	7.6	11.0	0.1	45.7
Sigaba	8.5	10.3	0.1	21.1
MailFilters	7.9	10.0	0.1	26.6
MessageGate	6.0	8.5	0.1	41.7
Adobe	6.1	8.3	0.1	36.1
Ubizen	7.2	8.2	0.1	13.2
Sendmail	5.0	8.0	0.1	60.0
Attachmate	6.2	7.5	0.1	19.9

TABLE 1

Worldwide Secure Content and Threat Management Revenue by Vendor, 2005–2006 ($M)

	2005	2006	2006 Share (%)	2005–2006 Growth (%)
SecureSoft	5.1	5.5	0.0	7.4
Tablus	3.4	5.0	0.0	47.1
LANDesk Software	4.2	4.8	0.0	15.2
Softforum	4.2	4.7	0.0	10.6
Akonix	3.5	4.5	0.0	28.6
Intrusion.com	4.0	4.2	0.0	5.0
Bull SAS	3.3	3.4	0.0	2.1
Oullim Information Technology	3.0	3.3	0.0	7.3
SSH Communications Security	3.2	3.2	0.0	0.0
Penta Security Systems	2.9	3.2	0.0	7.5
Webspy	1.1	1.3	0.0	17.9
Subtotal	9,192.1	10,331.1	78.0	12.4
Other	2,437.6	2,906.0	22.0	19.2
Total	11,629.7	13,237.1	100.0	13.8

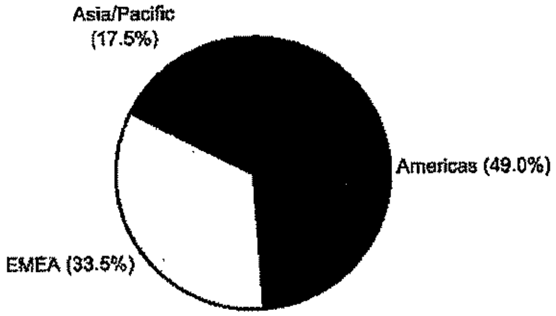
Source: IDC 2007

Performance by Geographic Region and Operating Environment in 2006

Worldwide SCTM revenue by region and operating environment is represented in Figures 2 and 3.

FIGURE 2

Worldwide Secure Content and Threat Management Revenue Share by Region, 2006

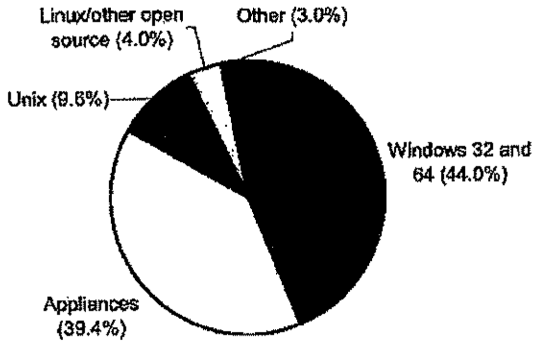


Total = $13.24B

Source: IDC, 2007

FIGURE 3

Worldwide Secure Content and Threat Management Revenue Share by Operating Environment, 2006



Total = $13.24B

Source: IDC, 2007

FUTURE OUTLOOK

Forecast and Assumptions

Secure Content and Threat Management Forecast, 2007–2011

Worldwide

IDC's estimate of the growth of the SCTM market through 2011 is presented in Table 2. IDC forecasts the SCTM market to grow from $13.2 billion in 2006 to $23.1 billion in 2011, representing an 11.8% compound annual growth rate (CAGR). Table 3 shows the key assumptions underlying this forecast.

TABLE 2

Worldwide Secure Content and Threat Management Revenue by Region and Operating Environment, 2006–2011 ($M)

	2006	2007	2008	2009	2010	2011	2006 Share (%)	2006–2011 CAGR (%)	2011 Share (%)
Geographic region									
Americas	6,486	7,430	8,497	9,525	10,430	11,322	49.0	11.8	49.0
EMEA	4,431	5,014	5,610	6,223	6,891	7,465	33.5	11.0	32.3
Asia/Pacific	2,320	2,675	3,054	3,443	3,846	4,338	17.5	13.3	18.8
Total	13,237	15,119	17,160	19,191	21,186	23,125	100.0	11.8	100.0
Operating environment									
Mainframe	28	28	29	29	29	28	0.2	0.3	0.1
i5 and OS/400	6	4	4	4	4	3	0.0	-11.1	0.0
Unix	1,269	1,407	1,483	1,549	1,609	1,654	9.6	5.4	7.2
Linux/other open source	536	498	623	778	964	1,182	4.0	17.1	5.1
Other host/server	206	215	226	221	218	213	1.6	0.6	0.9
Windows 32 and 64	5,825	6,752	7,489	8,076	8,765	9,412	44.0	10.1	40.7
Embedded	22	15	14	13	12	11	0.2	-12.3	0.0
Other single user	128	134	135	138	137	136	1.0	1.1	0.6
Appliances	5,217	6,065	7,156	8,383	9,427	10,487	39.4	15.0	45.3
Total	13,237	15,119	17,160	19,191	21,166	23,125	100.0	11.8	100.0
Growth (%)	NA	14.2	13.5	11.8	10.3	9.3			

Note: See Table 3 for key forecast assumptions.

Source: IDC, 2007

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Macroeconomics				
IT governance and regulatory compliance	Compliance is still driving some IT spending, including Sarbanes-Oxley, Basel II, and HIPAA. We don't expect compliance spending to crowd out other IT initiatives; in fact, compliance record keeping could spur initiatives in other areas as companies clean up their act. Increased attention to sound IT governance policies and compliance with regulatory requirements will drive an increased focus on storage and data management.	**Moderate.** Compliance and governance will have a positive impact on spending on infrastructure software that aids in the archiving, protection, and recovery of data. Compliance spending seems to be funding itself through better run business operations.	↑	★★★★☆
Economy	IDC assumes that worldwide and regional economic growth will be lower in 2007 compared with 2006. The United States will fall below 3%; Western Europe will come in at under 2%; and Latin America, Eastern Europe, and Asia/Pacific (excluding Japan) will all drop. While Japan is expected by Consensus Economics to hit 1.8%, IDC analysts in Japan believe the country will beat expectations.	**Moderate.** The economy — in its stability but lower growth — is now a net-neutral influence on IT spending. It does seem able to withstand oil shocks and terrorism.	↔	★★★★☆
Profits	2007 profits will be far less than 2006's estimated 19% growth, according to Consensus Economics' October 2006 poll — in fact, at 4%. IDC expects that profits will be lower, but not *that* low.	**Moderate.** IT spending is almost to full strength as company profits have been good for a few years. With high profits, organizations increased IT spending. As profits fall, enterprises will now be looking for cost savings. Security and risk management initiatives could benefit as improved IT operations are used as a productivity multiplier.	↔	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Policy	Compliance with government regulations, including Sarbanes-Oxley, GLBA, and HIPAA, and industry standards such as PCI is driving increased spending on IT. Much of that spending has been on services, but we expect enterprises to automate (with software) many compliance practices. Compliance record keeping could spur initiatives in other areas as companies clean up their act.	**High.** Compliance initiatives are the major driver for the security and vulnerability market. As more regulations proliferate, it becomes more difficult to manage the process manually, so software solutions are required. Enforcing and maintaining compliance means that all SVM product submarkets benefit.	↑	★★★★☆
Technology/ service developments				
Dynamic IT	IDC has identified the next style of computing — dynamic IT for dynamic enterprises — as a style that dramatically increases the effectiveness of IT. Within dynamic IT are a number of important subtrends — virtualization in the datacenter, data federation, software as a service (SaaS), and composite and rule-based applications. IDC assumes the transition to dynamic IT will be slow and labored, but will proceed nonetheless.	**Moderate.** Dynamic IT, by adding coherence to the enterprise usage of IT, would spur the market. However, confusing choices for enterprises and funding hurdles for new infrastructure will balance this impetus to market growth.	↔	★★★★☆
Killer apps	No killer apps or new technologies will come to drive overall industry growth in the same way Windows and office suites did in the 1980s or the Internet did in the late 1990s.	**Moderate.** With no killer app, enterprises will work to improve the security of their existing infrastructure.	↑	★★★★★

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Convergence	Convergence is a complex phenomenon working at many levels — convergence of the telephone network and the Internet; of communications and IT technologies; of consumer and enterprise technologies; and even of storage, routing, and processing in the datacenter. Of these, perhaps the most overarching is the convergence of voice, video, and data communications. IDC assumes that this convergence is a permanent phenomenon and that it will pick up pace as the decade wears on. One measure — by 2009, IDC expects 1.5 billion users on the Internet and 3 billion users of the phone network. With 2.5 billion mobile users, the overlap will be significant.	**High.** The extension of IT product lines into consumer electronics adds to overall market opportunity for IT vendors and expands the definition of the market. A number of security start-ups hope to tap the consumer market. As technology expands, the requirements to manage risk will also grow. Expect to see new security solutions that attempt to manage the risk associated with converged networks.	↑	★★★☆☆
Innovation	Vendors will continue security software, hardware, and services innovation at the same rate as in the past.	**Low.** The security market will not face bottlenecks from lack of new product development.	↔	★★★★☆
Enterprise workplace	Portal, collaboration, and content technologies will be applied in creative new ways to render "composite" applications that are more oriented toward specific user or user-role needs than as a prepackaged set of business processes.	**High.** The broadening of the enterprise workplace has greatly increased risk, and IT organizations are trying to manage this new environment. This will eventually require more usage of policy, compliance, forensics, patching, and vulnerability assessment tools.	↑	★★★★★

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Software industry transformation	The software industry is going through a major transformation, including basic architecture (SOA), the way software is written (composite applications), and the way software is delivered (SaaS) and even funded (advertising based). IDC assumes that this transformation will take a decade but that it will, when done, allow for much faster and more dynamic delivery of software functionality.	**Moderate.** The new software creation and delivery models should allow for a quantum increase in the ability to deliver and integrate new software functionality to IT&C systems. This should increase overall spending, even as it lowers costs.	↑	★★★☆☆
Software security	Software is becoming much more dangerous. Hackers and others continue to find ways to misuse other people's software. Initially this was done by exploiting a vulnerability, but they are now finding ways to misappropriate software without a known vulnerability.	**High.** Inherent software vulnerabilities or intentional software exploits are a dangerous trend that requires remediation, both during software development and after the fact. There is a growing awareness of the need to utilize software and application security tools during software development and deployment. Discovery, patching, and remediation remain important enterprise IT activities.	↑	★★★★★
Storage management	Storage management functions such as virtualization, migration, policy-based classification, and data movement will continue to evolve to aid in managing increasing amounts of data.	**Moderate.** More intelligent and automated ways to manage data resident on storage makes tiered storage more effective, but can also expand risks. The security of the storage level must be increased and managed.	↑	★★★★☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Pervasive computing (for mobile category)	This term refers to the proliferation of client devices and end-user or end-use devices at the network edge. By 2009, IDC expects five times as many non-PC devices to be connected to networks as PCs — including converged cell phones, networked entertainment and gaming devices, automobiles, building automation systems, and industrial controllers. This doesn't even count RFID tags and sensors. IDC assumes that communicating client devices will proliferate at 5 to 10 times the rate of PCs installed. Devices will both converge (cell phones with more functionality) and diverge (single-use devices, such as RFID readers).	**Moderate.** The addition of billions of devices to the network edge will drive the need for more enterprise systems to deploy, manage, and make use of them. It will also shift the prevailing traffic from the center of the network outward to edge-inward, which will affect computing and communications architectures.	↑	★★★★☆
Modular IT/risk aversion	Many firms remain cautious with regard to major IT investment/project implementation and have shifted to a more modular approach, with longer periods of testing and slower rates of decision-making implementation.	**Moderate.** Overall, demand will still fluctuate in the face of macroeconomic drivers/inhibitors, but the market should be less volatile. Large firms are taking a more long-term approach to IT than in previous years.	↔	★★★☆☆
Storage management	Storage management functions such as virtualization, migration, policy-based classification and data movement will continue to evolve to aid in managing increasing amounts of data.	**Moderate.** More intelligent and automated ways to manage data resident on storage helps to mitigate the problem of a fixed quantity of human resources and allows users to leverage tiered storage more effectively.	↑	★★★★☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Security delivery model	Security software is more likely to be delivered as a service and/or a security appliance than it will be bought as shrink-wrapped products.	**Moderate.** It will become more difficult to segment what is pure security software, what is inherent in a security appliance, and what is delivered as a software service. This has considerable impact on licensing and maintenance. Vendors like it because of the incremental revenue, and hardware vendors like it because they can provide solutions not available to them or leverage their appliances to create a revenue stream.	↑	★★★☆☆
Security threat environment	Software is becoming more rather than less vulnerable. Hackers and others continue to find ways to misuse other people's software. Initially, this was done by exploiting a vulnerability, but they are now finding ways to just misappropriate software without a vulnerability.	**High.** The ability to bury malware within other software will become a dangerous trend that will lead to improved spyware software and increase the need for software and application security tools at software development and deployment. It will also increase the need for intrusion prevention software that enforces application execution. Although great for the security market, it could have a dampening impact on software in general.	↑	★★★☆☆
Virtual machine software	Virtual machine software will cause a consolidation of physical machines and a proliferation of virtual machines.	**Moderate.** Virtual machine software is not expected to have a negative impact on operating systems images and may cause either some level of proliferation or an extension of the life expectancy, but without a related growth in revenue.	↓	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Launch of Windows Vista and Windows Longhorn Server	Windows Vista's broad launch in January 2007 will drive consumers to move to Windows Vista Home from Windows XP within days or weeks, but corporate adoption will follow a traditionally slower adoption ramp, due to application compatibility testing, compliance testing, IT and end-user training, and the lack of a critical mass of Windows Vista–ready machines within the installed base. Windows Longhorn Server, likewise, will be adopted on a timeline established by corporate IT practices, generally adopted as existing systems are retired and replaced, or when net-new machines are deployed.	**Moderate.** It will be "business as usual" for the Windows product shipments, with no significant "bump" of acquisitions or deployment immediately following the launch of Windows Vista or Windows Longhorn Server.	↔	★★★★★
Software complexity	Advances in standards and application infrastructure (such as SOA), while making it easier to build high-quality software, also add considerably to the complexity of resultant applications.	**High.** Complexity can work to the advantage of a vendor that provides an application or tools that promises to reduce complexity. However, indiscriminant and uncoordinated development of standards can have the opposite effect. Complexity also works to the advantage of large vendors that provide a single "integrated" software stack and is one of the key forces driving industry consolidation.	↓	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Standards	Standards provide recognition and approval of specifications regarding data and/or process. Standards will accelerate the use of technology.	**High.** Standards have the potential to affect a high degree of industry change. While standards curtail competition pertaining directly to the standard, they also foster competition in areas derivative to the standard. While standards are largely perceived to be a good thing, the indiscriminant creation of standards could lead to inconsistency, thereby undermining vendor credibility.	↑	★★★★☆
Consolidation	Consolidation will focus power in the hands of a small number of very large vendors.	**Moderate.** Consolidation is inevitable, but it is unclear if consolidation is good or bad. Consolidation is good because it encourages broad-based vertical or horizontal integration, which tend to reduce perceived developer or end-user complexity. However, consolidation also can serve to reduce competition and therefore slow the pace of evolutionary market change. Consolidation is a relatively new phenomenon in the software industry, so while its effects are not yet well understood, industry change appears to be accelerating and innovation (e.g., Google) continues.	↔	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Enterprise workplace	Portal, collaboration, and content technologies will be applied in creative new ways to render "composite" applications, but more oriented toward specific user or user-role needs than as a prepackaged set of business processes.	**High.** The enterprise workplace will offer a quick route to composite applications, which will be viewed by buyers as superior solution alternatives to old-fashioned "module" applications. The flexibility of "business integration on the glass" will drive buyers to switch budgets toward these types of efforts. Though underlying module prices may decrease (since users are only using pieces of those modules), the overall spend should increase and drive interest in this new class of offerings.	↑	★★★☆☆
On-demand applications	The software industry is going through a major transformation, including basic architecture (SOA), the way software is written (composite applications), and the way software is delivered (SaaS) and even funded (advertising based). IDC assumes that this transformation will take a decade but that it will, when done, allow for much faster and more dynamic delivery of software functionality. Vendors offering infrastructureless applications, aka on demand, will continue to garner share from license only–oriented vendors, and this phenomenon will spread to other applications beyond, for example, Web conferencing and sales automation.	**Moderate.** On-demand application specialists will force license-only suppliers to rethink their product delivery and licensing strategies and change their delivery to include on demand and offer new licensing options. Most application providers already offer "hosted" choices, so that is not a major impact. Though, overall, on demand may decrease prices at the outset of a new application sale, over the long run, it is not clear that vendors will recognize lower revenue, and the on-demand trends will reach new buyer audiences that could not afford classic license applications.	↑	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Market characteristics				
Hardware	Hardware markets continued to defy gravity and remained positive in 2006. IDC expects about the same performance in 2007, with pockets of both growth and decline. IDC assumes 6–7% growth in IT hardware spending (including network equipment sold to carriers and enterprises) in 2007.	**Moderate.** Hardware spending, about 40% of total IT spending, drives spending as well in software and services.	↔	★★★★☆
Software	The software market will remain a mix of slow-growth and high-growth markets. Business-oriented software — collaboration, messaging, analytics, and business metrics — are higher growth than most infrastructure-related software, with the exception of security. IDC assumes worldwide software spending in 2007 will be 8%.	**Moderate.** Software spending, about 20% of total IT spending, can drive spending in both hardware and IT and business services.	↔	★★★☆☆
Services	IT services will grow, but at a muted rate as companies implement smaller, quicker-payback projects. Price declines are expected as offshore sourcing and blended models (offshore, nearshore, onshore) increase. IDC expects worldwide IT services spending growth of 6% in 2007.	**Moderate.** IT services spending can affect the rate of overall solution adoption, as well as the migration to dynamic IT. It accounts for about 40% of IT spending.	↔	★★★★☆

TABLE 3

Key Forecast Assumptions for the Worldwide Secure Content and Threat Management Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
The Internet	Internet adoption is still going strong, especially in emerging economies. In the next four years, 500,000,000 new users will come online and commerce will double. By the end of 2006, over 50% of Internet households will be broadband. The hype around Web 2.0 is aiding awareness that the Internet economy is not dead.	**High.** Analysts and pundits may underestimate the impact of the Internet because the buzz is gone, despite the hype over Web 2.0. It will be an enabler for both new markets and new business models.	↑	★★★★☆

Legend: ★☆☆☆☆ very low, ★★☆☆☆ low, ★★★☆☆ moderate, ★★★★☆ high, ★★★★★ very high

Source: IDC, March 2007

By Geographic Region

IDC analysts around the globe supplied regional input and insight into the SCTM market forecast. The worldwide forecast is the aggregation of this regional data (refer to Table 2). Revenue for 2006 and 2011 is shown graphically in Figure 4.

By Operating Environment

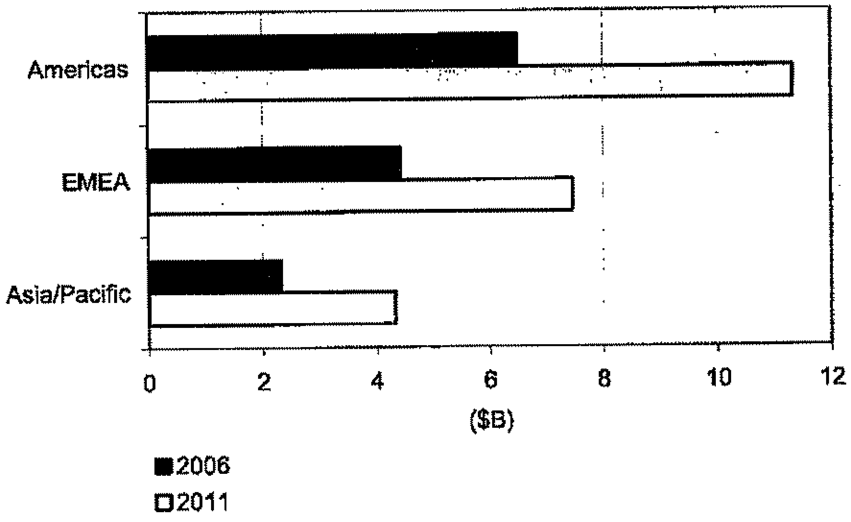
This study represents IDC's operating environment forecast for the SCTM market through 2011. For the revenue forecast for the SCTM market, segmented by operating environment, refer to Table 2; revenue for 2006 and 2011 is illustrated in Figure 5.

By Market Segment

IDC's estimate of the growth of the SCTM market by market segment is presented in Figure 6. We plan to publish individual market forecast and analysis studies to cover each of these market segments in more detail. These forthcoming reports will also include vendor market share and more granular segmentation of each market segment.

FIGURE 4

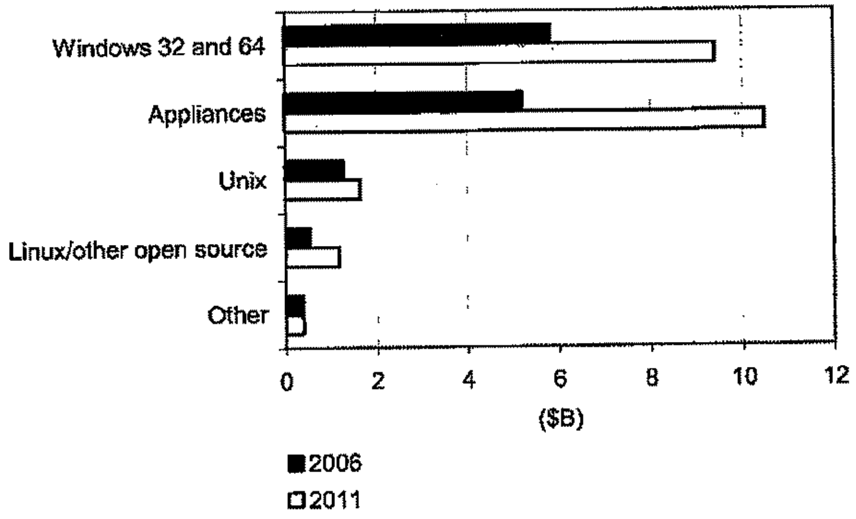
Worldwide Secure Content and Threat Management Revenue by Region, 2006 and 2011



Source: IDC, 2007

FIGURE 5

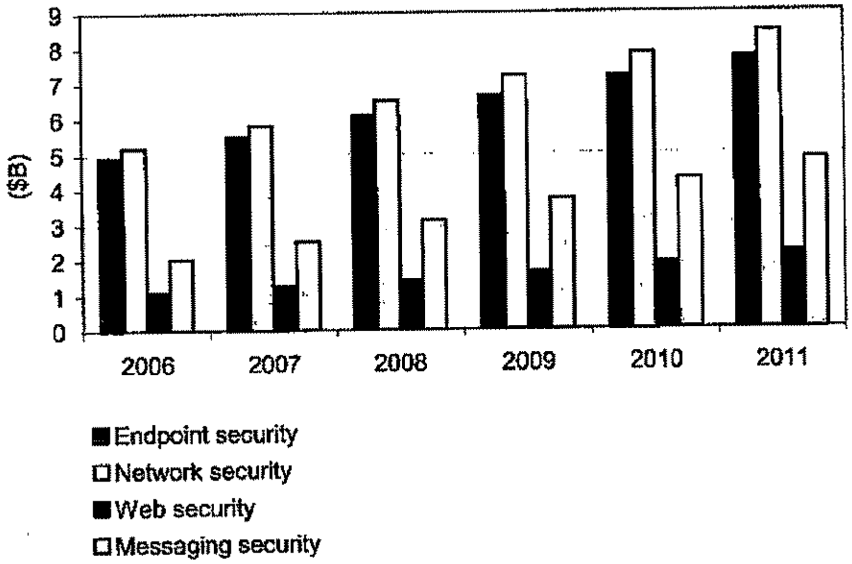
Worldwide Secure Content and Threat Management Revenue by Operating Environment, 2006 and 2011



Source: IDC, 2007

FIGURE 6

Worldwide Secure Content and Threat Management Revenue by Segment, 2006–2011



Source: IDC, 2007

ESSENTIAL GUIDANCE

The keys to success in the converged secure content and threat management market include consolidated management and tight integration. The ability to provide alerts and updates, aggregated logs, and common policy across various security technologies will be paramount. This will help organizations reduce the complexity of managing multiple products and, more important, lower the cost of administration. Consolidated management can make it easier for IT departments to better defend against new threats. For instance, with a single update for antivirus, firewall, and intrusion detection from a centrally managed console, corporations can respond faster to security threats and improve the overall security posture of the network.

An integrated approach is needed to deal with today's complex threat environment. Antivirus software works well to block known viruses. However, the increased sophistication of threats, such as blended threats, requires a new security approach. Moreover, with security vulnerabilities and new threats on the rise, integrated incident response techniques are key to preventing additional employees or corporate networks from being infected. If an attack is successful, an integrated incident response from a central management console becomes even more critical. From a financial perspective, the impact often involves employee downtime and the estimated replacement cost or value of lost, stolen, or destroyed corporate data.

IDC believes integrated SCTM solutions will be more effective in combating the complex new blended and hybrid threats than traditional deployment of independent security technologies.

Developments that will shape this market in the future include the following:

- **Network security.** Threat management security products remain a vital part of enterprise security when they can protect all aspects of the infrastructure. To this end, they are critical to enforcing network admission control (NAC). NAC utilizes products to cover the WAN, LAN, and endpoints. It will be up to threat management products to help enforce the NAC efforts, be it a network firewall that doesn't allow connectivity or establishes a VPN tunnel, an IPS that limits traffic, or an endpoint that watches application activity. Whatever the case, threat management products need to be tightly integrated into the NAC fabric. Vendors that already have their own NAC, partner with another company, or do a combination of both are already in a position to benefit from the growing interest in NAC. Those that are not connected will need to become connected. Network threat management software must be able to integrate with complementary security products, especially at the hardware level. Software vendors should look closely at licensing and partnering with security appliance and networking vendors. At the endpoint level, the vendors are already moving in the direction the market is moving toward: centrally managed integrated endpoint security products. For application protection, vendors must remain knowledgeable of the types of tools and exploits used by attackers.

- **Endpoint security.** Over the next few years, IDC would expect that the separate desktop antivirus, desktop antispyware, desktop firewalls, and host intrusion prevention products will all be incorporated into an integrated endpoint security product. This endpoint security solution will not be a suite, which is generally considered a combination of individual products; rather, endpoint defenses will become a single product that can perform all of the tasks incorporated into the individual products. IDC talked about policy-enforced client security a few years ago, but it appears that this will soon be more fact than fiction. It will be up to the enterprise to set the policy that the product will enforce. The central management with a single client install will be appealing to companies that need to reduce complexity associated with endpoint security.

- **Messaging security.** Messaging security products must provide broad protection from a wide range of emerging threats to enterprise security. While antivirus and antispam remain the foundation of messaging security, growing concerns with data leakage and regulatory compliance are driving the need for a more complete messaging security solution. The growing number of high-profile incidents in which customer records, confidential information, and intellectual property were leaked (or lost/stolen) has created an explosive demand for messaging security solutions that protect against the deliberate or inadvertent release of sensitive information. However, with all the hype around data leakage, it is critical that messaging security vendors not take their eye off the effectiveness of their antispam capabilities. Spam currently ranks as the third-greatest threat to enterprise security, according to IDC's latest security survey (see *Enterprise Security Survey, 2006: The Rise of the Insider Threat*, IDC #204807, December 2006). IDC has heard from many organizations that first- and second-generation antispam technologies are becoming less effective against increasing the volume and sophistication of attacks. The fact that image-based spam eludes detection by many existing antispam solutions has created strong demand for more effective antispam products and services. This represents a great opportunity for messaging security vendors.

- **Web security.** The Web is quickly becoming the threat vector of choice for hackers, spyware, and virus writers. Given the real-time nature of Web traffic, more sophisticated real-time scanning capabilities are needed to ensure that traffic within these Web-based paths remains free from successful attacks through these vectors. The challenge Web security vendors have is in providing effective Web security without impacting the end user. IDC believes Web security solutions must address the performance and latency issues of traditional security solutions without sacrificing effectiveness and accuracy. Effective Web security solutions must deliver real-time performance in order to scan high volumes of Web traffic for spyware, viruses, worms, and other types of malicious code.

LEARN MORE

Related Research

- *Worldwide Mobile Device Security 2007–2011 Forecast* (IDC #206072, March 2007)
- *IDC's Software Taxonomy, 20076* (IDC #205437, February 2007)
- *Worldwide Threat Management Security Appliances 2006–2010 Forecast and 2005 Vendor Shares: Easing the Pain* (IDC #204841, December 2006)
- *Enterprise Security Survey, 2006: The Rise of the Insider Threat* (IDC #204807, December 2006)
- *Worldwide Threat Management Software 2006–2010 Forecast and Analysis: Full-Press Defenses* (IDC #204720, December 2006)
- *Worldwide Security and Vulnerability Management Software 2006–2010 Forecast and Analysis: Managing Security Knowledge and Control* (IDC #204693, December 2006)
- *Worldwide Secure Content Management 2006–2010 Forecast Update and 2005 Vendor Shares: The Convergence of Secure Content and Threat Management* (IDC #203550, September 2006)
- *Worldwide Security Compliance and Control 2006–2010 Forecast and Analysis: Going Beyond Compliance to Proactive Risk Management* (IDC #203350, September 2006)

Methodology

The IDC software market sizing and forecasts are presented in terms of "packaged software revenue." IDC uses the term *packaged software* to distinguish commercially available software from "custom" software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available through sale, lease, rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of the above are counted by IDC as packaged software revenue.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments.

The market forecast and analysis methodology incorporates information from five different but interrelated sources, as follows:

☒ **Reported and observed trends and financial activity.** This study incorporates reported and observed trends and financial activity in 2006 as of the end of April 2007, including reported revenue data for public companies trading on North American stock exchanges (CY 1Q06–4Q06 in nearly all cases).

☒ **IDC's *Software Census* Interviews.** IDC interviews all significant market participants to determine product revenue, revenue demographics, pricing, and other relevant information.

☒ **Product briefings, press releases, and other publicly available information.** IDC's software analysts around the world meet with hundreds of software vendors each year. These briefings provide an opportunity to review current and future business and product strategies, revenue, shipments, customer bases, target markets, and other key product and competitive information.

☒ **Vendor financial statements and related filings.** Although many software vendors are privately held and choose to limit financial disclosures, information from publicly held companies provides a significant benchmark for assessing informal market estimates from private companies. IDC also builds detailed information related to private companies through in-depth analyst relationships and maintains an extensive library of financial and corporate information focused on the IT industry. We further maintain detailed revenue by product area models on more than 1,000 worldwide vendors.

☒ **IDC demand-side research.** This includes thousands of interviews with business users of software solutions annually and provides a powerful fifth perspective for assessing competitive performance and market dynamics. IDC's user strategy databases offer a compelling and consistent time-series view of industry trends and developments. Direct conversations with technology buyers provide an invaluable complement to the broader survey-based results.

Ultimately, the data presented in this study represents IDC's best estimates based on the above data sources as well as reported and observed activity by vendors and further modeling of data that we believe to be true to fill in any information gaps.

The data in this study is derived from all the above sources and entered into the Software Market Forecaster (SMF) database, which is then updated on a continuous basis as new information regarding software vendor revenues becomes available. For this reason, the reader should note carefully the "as of" date in the Methodology discussion within the In This Study section, near the beginning of this study, whenever making comparisons between the data in this study and the data in any other software revenue study.

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Published Under Services: Secure Content and Threat Management Products

EXHIBIT 28

SOURCE: Secure Computing Corporation

Mar 28, 2008 09:00 ET

Secure Computing Files Motion to Set Aside Previous Infringement Verdict

Secure Computing to Oppose Finjan's Request for an Injunction

Highlighted Links

Secure Home Page

SAN JOSE, CA--(Marketwire - March 28, 2008) - Secure Computing Corporation (NASDAQ: SCUR), a leading enterprise gateway security provider, today announced that its Webwasher products will continue to be available to protect against Web-borne threats. Secure Computing filed a motion in the District Court in Delaware on March 26th to set aside the jury verdict of infringement and to enter judgment that Finjan's patents are invalid and are not infringed by any Secure Computing product. Secure Computing will oppose Finjan's request for an injunction.

"We do not believe that we infringe any of Finjan's patents, and we believe Finjan's patents are invalid," said Mike Gallagher, Secure Computing's senior vice president, product development and support. "We will oppose all efforts by Finjan to limit the availability of Webwasher, a product that we believe provides superior protection against Web-borne threats. We hope and expect the courts will reject Finjan's request for an injunction to limit the availability of a small set of functions in Webwasher while they consider the validity of Finjan's patents. But we do have plans in place to address the specific functions that Finjan has targeted that will allow us to continue to sell and support Webwasher in any event."

Secure Computing previously announced on March 13, 2008 that Secure Computing does not believe that it infringes upon Finjan's patents in any way, and the Company further believes that Finjan's patents are invalid. Webwasher's proactive scanning technology accused of infringement by Finjan uses heuristic rules to categorize the behavior of executable code. The use of heuristics in general to analyze code was known and in use prior to the filing of any of Finjan's patents. The specific complex heuristics in the proactive scanning module were developed by Webwasher and are the product of Webwasher's original research. Secure Computing has requested that the trial court set aside the jury verdict and, if necessary, the Company intends to appeal to the Federal Circuit Court of Appeals.

Secure Computing's separate patent infringement suit against Finjan's load balancing technology remains pending in the District Court for the Federal District of Delaware.

"The District Court Judge in Delaware has not had any opportunity yet to rule on the validity of Finjan's patents, an opportunity the Court will now have based on the motion we have filed today," said Mary Budge, senior vice president, secretary and general counsel, Secure Computing. "We firmly believe that we have substantial grounds for relief in the trial court, and if necessary, for appeal, and we intend to proceed with the suit against Finjan on our load balancing patent. We are extremely motivated to challenge this result and we plan to take all the necessary steps to over-turn it."

About Secure Computing Corporation

Secure Computing Corporation (NASDAQ: SCUR), a leading provider of enterprise gateway security, delivers a comprehensive set of solutions that help customers protect their critical Web, email and network assets. Over half the Fortune 50 and Fortune 500 are part of our more than 22,000 global customers, supported by a worldwide network of more than 2,000 partners. The company is headquartered in San Jose, Calif., and has offices worldwide. For more information, see http://www.securecomputing.com.

This press release contains forward-looking statements relating to the appeal to the Federal Circuit Court of Appeals and any potential outcome or result of such statements involve a number of risks and uncertainties. Among the important factors that could cause actual results to differ materially from those indicated by such forward-looking statements are the likelihood of success at the trial court and at the appellate level, general economic conditions and the risk factors detailed from time to time in Secure Computing's periodic reports and registration statements filed with the Securities and Exchange Commission.

UK)

EXHIBIT 29

+1.800.379.4944 Toll Free
+1.408.979.6572 International

Select Language

Resources Products Try/Buy Support Partners Company Search

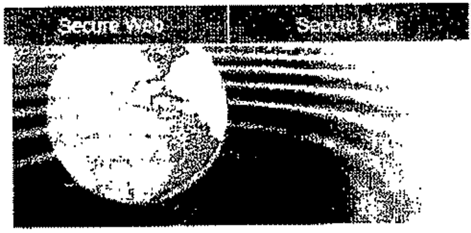
Resources Products Try/Buy

Locator

Printable Version

Home > Support > Technical Support >> Product Life Cycle Information

Secure Web | Secure Mail | Secure Firewall | Secure SafeWord®



Next Steps

Attend a Webinar

Technical Support

Product Life Cycle Information

Generally, Secure Computing® provides technical support on our products as it relates to the hosting platform for three (3) years. This is to ensure that our support-services customers can be confident that we will have a supported version of our software available for their operating system, host application, or appliance platform for typically no less than three years from the date that the product first shipped.

Secure Computing maintains a product life cycle program to ensure our customers clearly understand the support status of their Secure Computing products at all times. Policies related to product life stages vary by product. Appliances, for example, have different life cycle characteristics than do pure software products or than do subscription-based services like URL filtering or anti-virus updates. Our product life cycle programs assume that our customers stay relatively current with the latest released version of our products, and upgrade their Secure Computing software as new releases become available.

Product Life Cycle Charts

The following charts detail the product life cycle support status of Secure Computing's products.

- **Identity and Access Management**
  - **SafeWord® versions**
  - **SecureWire™**
- **Network Gateway Security (UTM/Firewall/VPN)**
  - **Sidewinder®**
    - **Sidewinder Anti-Spam Add-On Module**
    - **Sidewinder SoftRemote Add-On Module**
  - **SecurityReporter™**
  - **Secure CommandCenter™**
  - **Sidewinder G2® Enterprise Manager**
  - **CyberGuard® Classic**
  - **CyberGuard® TSP**
  - **SnapGear®**
  - **Gauntlet™**
  - **Global Command Center™ (GCC)**
- **Web Gateway Security**
  - **Webwasher® Web Gateway Security Appliance**
  - **Webwasher®**
  - **SmartFilter®**
  - **Internet Database of Categorized Content**
  - **N2H2 Bess® and Sentian™**
  - **ZIX Message and Web Inspector**

Support

- Activations
- Downloads
- Customer Service
- Technical Support
- Online Support Login
- Knowledge Base
- Support Certificate
- Call Statistics
- Warranties and agreements
- **Product Life Cycle Information**
- Training

- **Messaging Products**

Contact **Customer Service** with questions, or to receive future support announcements regarding product status.

Life Stage Descriptions

- **ACTIVE Status**
  Products identified with the Active status are currently orderable and no last order date has been published. The product is fully supported by Secure Computing.

  Recommendation: Purchase

- **LOD Status**
  Products identified with the LOD status have a published last order date or they may have in fact passed the last order date. The product is fully supported by Secure Computing.

  Recommendation: Make last purchase or plan for upgrade

- **MAINTENANCE Status**
  Products identified with the Maintenance status have a published end of life date and will continue to be supported with minor fixes & patches but will not receive any new feature enhancements.

  Recommendation: Upgrade as soon as possible

- **EOL Status**
  Products identified with the EOL status have a published end of life date and they have past their end of life date. The product is no longer supported under Secure Computing agreements. No new software releases for the product's platform (e.g., the host operating system, host application, or appliance platform) are planned, and no additional maintenance releases or patches will be made available.

  Recommendation: Must upgrade

Product Life Cycle Charts

The following charts detail the product life cycle support status of Secure Computing products.

Identity and Access Management

SafeWord® Strong Authentication Product List

Software/version	Status	LOD date	EOL date	Supported platforms
SafeWord® RemoteAccess™ 2.2	Active			WIN 2000, WIN 2003
SafeWord® RemoteAccess™ 2.1	LOD*	12/29/06		WIN 2000, WIN 2003
SafeWord® RemoteAccess™ 2.0	LOD*	09/30/05		WIN 2000, WIN 2003

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v2.2 for maintenance)*

SafeWord® RemoteAccess™, Cisco Compatible 2.2	Active			WIN 2000, WIN 2003
SafeWord® RemoteAccess™, Cisco Compatible 2.1	LOD*	12/29/06		WIN 2000, WIN 2003
SafeWord RemoteAccess™, Cisco Compatible 2.0	LOD*	09/30/05		WIN 2000, WIN 2003

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v2.2 for maintenance)*

SafeWord® for Citrix® 2.2	Active			WIN 2000, WIN 2003
SafeWord® for Citrix® 2.1	LOD*	12/29/06		WIN 2000, WIN 2003
SafeWord® for Citrix® 2.0	LOD*	09/30/05		WIN 2000, WIN 2003
SafeWord® for Citrix® 1.1	LOD*	12/18/03		WIN 2000

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v2.2 for maintenance)*

SafeWord® for Check Point 2.2	Active			WIN 2000, WIN 2003
SafeWord® for Check Point 2.1	LOD*	12/29/06		WIN 2000, WIN 2003
SafeWord® for Check Point 2.0	LOD*	09/30/05		WIN 2000, WIN 2003

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v2.2 for maintenance)*

SafeWord® for Nortel Networks 2.2	Active			WIN 2000, WIN 2003
SafeWord® for Nortel Networks 2.1	LOD*	12/29/06		WIN 2000, WIN 2003
SafeWord® for Nortel Networks 2.0	LOD*	09/30/05		WIN 2000, WIN 2003

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v2.2 for maintenance)*

SafeWord® PremierAccess® 4.0	Active			WIN 2000, WIN 2003, SOL 9-10
SafeWord® PremierAccess® 3.2	Active			WIN 2000, WIN 2003, SOL 9-10
SafeWord® PremierAccess® 3.1.1	LOD*	12/31/04		WIN 2000, SOL 7-8
SafeWord® PremierAccess® 3.1	LOD*	11/27/02		WIN 2000, SOL 7-8
SafeWord® PremierAccess® 3.0	LOD*	05/31/02		WIN 2000, SOL 7-8

***Note:** *The above LOD versions are past LOD, in support, (Must upgrade to v4.0 or v3.2 for maintenance)*

SafeWord Plus™ 2.1.1	EOL		01/31/06	SOL 7
SafeWord Plus™ 2.1	EOL		01/31/06	SOL 7
SafeWord Plus™ 2.0	EOL		01/31/06	SOL 7
SafeWord® AS 5.x	EOL		12/31/02	WINNT4, SOL 2.5-7, HPUX11

Patches and upgrades >>

SecureWire Product List

Model	Status	LOD date	EOL date	Original release	Comments
2500	ACTIVE			3.0.0	
500	ACTIVE			3.0.0	
100	ACTIVE			3.0.0	

Network Gateway Security (UTM/Firewall/VPN)

Sidewinder® (G2)

Note: These tables for Sidewinder G2 below, reflect product life cycle status for major product version and their updates, up to 3 decimal points (e.g. 6.1.1). Beginning in November 2005, the life cycle support information for patch levels (e.g. 6.1.1.03) will be noted in the release notes for each patch.

Sidewinder® (G2) Software Only - for customers running on a hardware platform of their own choosing (i.e. not an appliance)

Version	Status	LOD date	EOL date	Comments
6.1.1.x	EOL	Not for sale, upgrade only	12/31/06	Software upgrades available until 3/31/06. All software only versions are EOL on 12/31/06. Please inquire about special discounts on appliance upgrades.
6.1.0.x	EOL	Not for sale, upgrade only	12/31/06	Software upgrades available until 6/30/05. All software only versions are EOL on 12/31/06. Please inquire about special discounts on appliance upgrades.

6.0.x	EOL	6/30/04	2/1/06	-
5.2.x	EOL	3/31/03	12/31/04	-
5.1.x	EOL		2/28/03	-
5.0.x	EOL		6/30/02	-

Sidewinder and Sidewinder G2 patches are available here >>

Sidewinder® (G2) - Appliance Hardware

Model	Status	LOD date	EOL date	Original release	Compatible & Supported versions	Replacement Model
110 D	ACTIVE			6.1.2.01	6.1.2.01 or higher	
210 D	ACTIVE			6.1.2.01	6.1.2.01 or higher	
410 D	ACTIVE			6.1.2	6.1.2 or higher	
510 D	ACTIVE			6.1.2	6.1.2 or higher	
1100 D	ACTIVE			6.1.2.02	6.1.2.02 or higher	
2100 D	ACTIVE			6.1.2.02	6.1.2.02 or higher	
2150 D	ACTIVE			6.1.2.02	6.1.2.02 or higher	
4150 D	ACTIVE			6.1.2.02	6.1.2.02 or higher	
110 C	LOD	9/30/06		6.1.0.05	6.1.0.05 or higher	110 D
210 C	LOD	9/30/06		6.1.0.05	6.1.0.05 or higher	210 D
410 C	LOD	4/30/06		6.1.0.05	6.1.0.05 or higher	410 D
510 C	LOD	4/30/06		6.1.0.05	6.1.0.05 or higher	510 D
1100 C	LOD	12/31/06		6.1.1.01	6.1.0.01 or higher	1100 D
2100 C	LOD	12/31/06		6.1.0.05	6.1.0.05 or higher	2100 D
2150 C	LOD	12/31/06		6.1.0.05	6.1.0.05 or higher	2150 D
4150 C	LOD	12/31/06		6.1.1.01	6.1.0.01 or higher	4150 D
1100 B	LOD	6/30/05		6.1.0.05	6.1.0.05 or higher	
4150	LOD	5/1/05		6.1	6.1 or higher	
210	LOD	3/15/05		6.1	6.1 or higher	
310a	LOD	10/31/04		6.1	6.1 or higher	
310b	LOD	3/15/05		6.1.0.04	6.1.0.04 or higher	
315	LOD	3/15/05		6.1	6.1 or higher	
410a	LOD	10/31/04		6.1	6.1 or higher	
410b	LOD	3/15/05		6.1.0.04	6.1.0.04 or higher	
415	LOD	3/15/05		6.1	6.1 or higher	
510/515	LOD	3/15/05		6.1	6.1 or higher	
1100/1150	LOD	3/15/05		6.1	6.1 or higher	
2100	LOD	3/15/05		6.1	6.1 or higher	
2150	LOD	3/15/05		6.1	6.1 or higher	
25a	LOD	8/31/02		5.2.1	6.1 or higher (6.1 upgrade requires min. 512 MB RAM) 6.0 EOL as of 2/1/06	
25b	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06	
100	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06	
250	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06	

1000a	LOD	12/31/02		5.2.1	6.1 or higher (6.1 upgrade requires min. 512 MB RAM) 6.0 EOL as of 2/1/06
1000b	LOD	9/30/03		6.0	6.1 or higher 6.0 EOL as of 2/1/06
1000c	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06
2000a	LOD	9/30/03		6.0	6.1 or higher 6.0 EOL as of 2/1/06
2000b	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06
4000	LOD	3/31/04		6.0	6.1 or higher 6.0 EOL as of 2/1/06

Sidewinder® (G2) - Appliance Software

Version	Status	LOD date	EOL date	Comments
7.0.0	ACTIVE			v7.0 is not available for Sidewinder G2 Enterprise Manager
6.1.2	LOD	12/31/2007	12/31/2009	
6.1.1.x	MAINTENANCE	3/31/06	4/30/08	
6.1.0.x	MAINTENANCE	6/30/05	9/30/07	
6.0.x	EOL	6/30/04	2/1/06	
5.2.1	EOL	3/31/03	12/31/04	

Sidewinder and Sidewinder G2 patches are available here >>

Sidewinder Anti-Spam Add-On Module

Version	Status	LOD date	EOL date	Comments
All versions	MAINTENANCE	12/31/2007	12/31/2008	Subscription may be renewed only through 12/31/2008 via the pro-rated price.

TrustedSource™, Secure Computing's proactive reputation-based security technology is now bundled for FREE with Sidewinder v7 in 2008.

Sidewinder SoftRemote Add-On Module

Version	Status	LOD date	EOL date	Comments
All versions	MAINTENANCE	12/31/2007	12/31/2008	Support may be renewed only through 12/31/2008 via the pro-rated price.

The SoftRemote IPSec VPN Client can now be purchased directly through SafeNet. See URL: **http://www.safenet-inc.com/softremote/index.asp**

CommandCenter - Appliance Hardware

Model	Status	LOD date	EOL date	Original release	Compatible & Supported versions
CC500	ACTIVE			4.0	4.0 or higher
CC1500	ACTIVE			4.0	4.0 or higher
CC2500	ACTIVE			4.0	4.0 or higher

CG2800	ACTIVE			4.0	4.0 or higher

CommandCenter - Appliance Software

Version	Status	LOD date	EOL date	Comments
4.0	ACTIVE			This product replaces Global Command Center for Sidewinder and Sidewinder Enterprise Manager. v4.0 is not available for SnapGear.

CommandCenter patches are available here >>

SecurityReporter - Software

Version	Status	LOD date	EOL date	Compatible & Supported versions
4.6.4	ACTIVE			Sidewinder v7.0 or higher, and Sidewinder G2 v6.1.1 or higher
4.6.3	MAINTENANCE	09/30/2007		Sidewinder v7.0 or higher, and Sidewinder G2 v6.1.1 or higher
4.2.30	MAINTENANCE	5/21/07		Sidewinder G2 v6.1.0.05 or higher
4.2.29	EOL	8/21/06	5/21/07	Sidewinder G2 v6.1.2 or higher

Sidewinder G2® Enterprise Manager - Appliance Hardware

Model	Status	LOD date	EOL date	Original release	Compatible & Supported versions
10 D	ACTIVE	12/31/07		6.1.2.02	6.1.2.02 or higher
25 D	ACTIVE	12/31/07		6.1.2.02	6.1.2.02 or higher
50 D	ACTIVE	12/31/07		6.1.2.02	6.1.2.02 or higher
UL D	ACTIVE	12/31/07		6.1.2.02	6.1.2.02 or higher
10 C	LOD	12/31/06		6.1.1.01	6.1.1.01 or higher
25 C	LOD	12/31/06		6.1.0.05	6.1.0.05 or higher
50 C	LOD	12/31/06		6.1.0.05	6.1.0.05 or higher
UL C	LOD	12/31/06		6.1.0.05	6.1.0.05 or higher
10	LOD	6/30/05		6.1	6.1 or higher
25	LOD	3/15/05		6.1	6.1 or higher
50	LOD	3/15/05		6.1	6.1 or higher
UL	LOD	3/15/05		6.1	6.1 or higher

Sidewinder and Sidewinder G2 patches are available here >>

Sidewinder G2® Enterprise Manager - Appliance Software

Version	Status	LOD date	EOL date	Comments
6.1.2	LOD	12/31/07	12/31/09	
6.1.1.x	MAINTENANCE	3/31/06	4/30/08	
6.1.0.x	EOL	6/30/05	3/31/07	
6.0.x	EOL	6/30/04	2/1/06	
5.2.1	EOL	3/31/03	12/31/04	

CyberGuard "Classic" Appliances

- All Classic software releases are EOL on December 31, 2007, however some Classic appliances can continue to be used (if they are eligible) and also make the upgrade to TSP or Sidewinder v7.0 software. Please check with your Secure Computing account manager or channel partner for more information about eligibility and upgrade options.
- Last Order Dates are represented as "while quantities last."
- Fulfillment will transition to replacement models if possible.
- When inventory depletion is complete the model will no longer be available for sale (Sold Out).

Model	Status	LOD date	EOL date	Original release	Compatible & Supported versions	Replacement Model
FS300	LOD	12/31/06		Classic v5.2	Classic v5.2	None
FS600	LOD	12/31/06		Classic v5.2	Classic v5.2	None
KS1000	LOD	12/31/06		Classic v5.2	Classic v5.2	KS1000-J
KS1500	LOD	12/31/06		Classic v5.2	Classic v5.2	KS1500-J
KS1500R	Sold Out	2/17/06		Classic v5.2	Classic v5.2	None
SL3200	Sold Out	2/17/06		Classic v5.2	Classic v5.2	None
KS1000J	LOD	12/31/06		Classic v5.2	Classic v5.2	None
KS1500J	LOD	12/31/06		Classic v5.2	Classic v5.2	None

CyberGuard Classic Appliance - Software

Version	Status	LOD date	EOL date	Comments
Classic (all versions)	MAINTENANCE	12/31/06	12/31/07	EOL will be 12/31/07

CyberGuard "TSP" Appliances

- TSP units will move to the Secure Computing common appliance platforms.
- Last Order Dates are represented as "while quantities last."
- When inventory is depleted, fulfillment will transition to replacement models.
- NO EOL dates have been announced for the TSP line.

Model	Status	LOD date	EOL date	Original release	Compatible & Supported versions	Replacement Model
TSP 110 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 210 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 410 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 510 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 1100 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 2100 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 2150 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 4150 D	ACTIVE	12/31/07		v6.4.1	v6.4.1 & higher	
TSP 7300	LOD	12/31/06		v6.4	v6.4 & higher	
TSP 7100	LOD	12/31/06		v6.4	v6.2 & higher	TSP 7300
TSP 5100	Sold Out	2/17/06		v6.2	v6.2 & higher	TSP 3450-J
TSP 3600	Sold Out	2/17/06		v6.2	v6.2 & higher	TSP 3450-J
TSP 3400	LOD	12/31/06		v6.2	v6.2 & higher	TSP 3400-J
TSP 3100	LOD	12/31/06		v6.2	v6.2 & higher	TSP 3100-J
TSP 1150	LOD	12/31/06		v6.2	v6.2 & higher	TSP 410 D
TSP 1250	LOD	12/31/06		v6.2	v6.2 & higher	TSP 510 D
TSP 3100-J	LOD	12/31/06		v6.2	v6.2 & higher	TSP 1100 D
TSP 3400-J	LOD	12/31/06		v6.2	v6.2 & higher	TSP 1100 D
TSP 3450-J	LOD	12/31/06		v6.4	v6.2 & higher	TSP 2150 D
TSP 7100	LOD	12/31/06		v6.2	v6.2 & higher	TSP 4150 D

CyberGuard TSP Appliance - Software

Version	Status	LOD date	EOL date	Comments
6.4.x	MAINTENANCE	12/31/07	12/31/09	
6.3.0	MAINTENANCE		12/31/08	Note: 6.3 was a restricted release and will EOL with 6.2.
6.2.x	MAINTENANCE		12/31/08	
6.1.3	EOL		7/2005	
6.1.2	EOL		4/2005	

6.1.1	EOL		12/2004	

SnapGear® Product List

Model	Status	LOD date	EOL date	Current SW version	Comments
SG720	ACTIVE			3.1.5u3	
SG710+	MAINTENANCE	12/2006	12/2008	3.1.5u3	
SG710	MAINTENANCE	12/2006	12/2008	3.1.5u3	
SG640	ACTIVE			3.1.5u3	
SG635	MAINTENANCE	12/2006	12/2008	3.1.5u3	
SG580	ACTIVE			3.1.5u3	
SG565	ACTIVE			3.1.5u3	
SG560	ACTIVE			3.1.5u3	
SG300	ACTIVE			3.1.5u3	
SG630	EOL	12/2005	12/2007	3.1.5u3	
SG575	EOL	06/2005	06/2007	3.1.5u3	
SG570	EOL	06/2005	06/2007	3.1.5u3	
SG550	EOL	06/2005	06/2007	3.1.5u3	
SG530	EOL	06/2005	06/2007	3.1.5u3	
Lite2+	EOL	12/2004	12/2006	1.8.10	
Lite2	EOL	12/2004	12/2006	1.8.10	

Gauntlet software

Version	Status	LOD date	EOL date
6.0	EOL	10/15/03	12/31/04
5.5	EOL		12/31/03
5.0	EOL		7/31/03

e-ppliance Gauntlet (all models)

Version	Status	LOD date	EOL date
2.0	EOL	10/15/03	12/31/04
1.5	EOL		12/31/03
1.0	EOL		7/31/03

Gauntlet patches are available here >>

Global Command Center - Software

Version	Status	LOD date	EOL date	Comments
3.2.x	LOD	3/31/08	12/31/09	After 12/31/2007, available only with orders of 50+ SnapGear units and 1 year of Support.
3.2	MAINTENANCE		3/1/08	
3.1	MAINTENANCE		12/31/07	
3.0	MAINTENANCE		6/1/07	
2.5.2	EOL		10/31/05	
2.5.1	EOL		3/31/05	
2.5	EOL		11/30/04	
2.0	EOL		6/30/04	

- Global Command Center (GCC) and Sidewinder G2 Enterprise Manager (EM) will be replaced by CommandCenter 4.0 appliance.
- Between now and the end of 2009 GCC and EM customers will migrate from Sidewinder G2 and TSP to

Sidewinder 7.0, which is centrally managed by CommandCenter 4.0. For roadmap details please contact your account manager or channel partner.

Web Gateway Security

Webwasher Web Gateway Security Appliance

Model	Status	LOD date	EOL date	Supported OS
WW2900B	Active			Proprietary
WW1900B	Active			Proprietary
WW1100B	Active			Proprietary
WW500B	Active			Proprietary
SME250B	Active			Proprietary
SME250	Maintenance	8/2007	8/2012	Proprietary
WW1900	Maintenance	6/2007	6/2012	Proprietary
WW1100	Maintenance	6/2007	6/2012	Proprietary
WW500	Maintenance	6/2007	6/2012	Proprietary
WW1000	LOD	12/2006	3/2010	Proprietary

Webwasher Product List

Software/version	Status	LOD date	EOL date	Supported platforms
Webwasher CSM Suite 6.6 † [1]	Active			Debian 3.1 & 4.0, RHES 3.0 & 4.0, Solaris 8[2], 9 & 10, SLES 8.0[2] & 9.0, WIN 20002 & 2003
Webwasher CSM Suite 6.5 † [1]	LOD	9/2007	6/2008	Debian 3.1 & 4.0, RHES 3.0 & 4.0, Solaris 8[2], 9 & 10, SLES 8.0[2] & 9.0, WIN 20002 & 2003
Webwasher CSM Suite 6.0 †[1]	LOD	3/2007	12/2007	Debian 3.1, RHES 3.0 or 4.0, Solaris 8, 9 or 10, SLES 8.0 or 9.0, WIN 2000 or 2003
Webwasher CSM Suite 5.3 † [1]	LOD	12/2006	12/2009	Debian 3.1, RHES 3.0 or 4.0, SLES 8.0[2] or 9.0, Solaris 8[2] or 9, WIN 2000[2] or 2003
Webwasher CSM Suite 5.2[#]	EOL	11/2005	12/2006	Debian 3.0 or 3.1, RHES 3.0, SLES 8.0 or 9.0, Solaris 8 or 9, WIN 2000 or 2003
Content Reporter 4.7 †*	Active			RHEL 4.0, SLES 9, Solaris 8 or 9 *, WIN 2000 or 2003. Support database versions: Oracle 8.1.7, Oracle 9i, or 10g, Microsoft SQL 2000 or 2005, MaxDB 7.5 (included)
Content Reporter 4.6 †	EOL	12/2006	06/2007	WIN 2000 or 2003, Linux, Solaris 7, 8 or 9. Support database versions: Oracle 8.1.7, Oracle 9i, Oracle 10g, Microsoft SQL 2000, MaxDB 7.5 (included)
Content Reporter 4.5	EOL	11/2005	12/2006	WIN 2000 or 2003, Solaris 7, 8 or 9. Support database versions: Oracle 8.1.7, Oracle 9i, Oracle 10g, Microsoft SQL 2000, MaxDB 7.5 (included)
Instant Messenger Filter 4.2 †	Active			WIN 2000 or 2003
Instant Messenger Filter 4.0	LOD	11/2005		WIN 2000 or 2003
Web Inspector 1.0 †	Active			WIN 2000, 2003 and XP PRO

[#] McAfee no longer provides Anti-Virus signature updates for WW v5.2 or older effective 1/31/2007

[1] For Computer Associates eTrust Anti-Virus module: LOD defined as of 9/2007 and EOL defined as of 12/2008

[2] EOL for this platform defined as of 12/2007

[*] Content Reporter is only supported on Solaris 64 bit OS

† Webwasher has not been tested on, and does not currently support 64-bit OS editions or hardware

SmartFilter Product List

Software/version	Status	LOD date	EOL date	Supported OS or application platforms
SmartFilter 3.x.x	EOL	7/2004	9/2006	Win 2000, RHL 7.2, RHL 9.0, Solaris 2.6 or 8
SmartFilter 4.0.x	EOL	9/2005	9/2007	Win 2000, Win 2003, RHL 7.3, RHL 9.0, Red Hat ES 3.0, Solaris 8 or 9
SmartFilter 4.1.x	LOD	06/2007	06/2008	Win 2000, Win 2003, Win XP Pro, RHL 9.0, Red Hat ES 3.0 or 4.0, Solaris 8 or 9
SmartFilter 4.1.1.02 - Cisco CE	LOD	06/2007	04/2008	
SmartFilter 4.1.1.01 - UFP (FW-1)	LOD	06/2007	06/2008	
SmartFilter 4.1.1.01 - Volera (IFP)	LOD	06/2007	06/2008	
SmartFilter 4.1.1.02 - Sidewinder 6.1.x	LOD	06/2007	12/2009	
SmartFilter 4.2.x	ACTIVE			Win 2000, Win 2003, Win XP Pro, Win Vista, Red Hat ES 3.0/4.0/5.0, Solaris 8/9/10
SmartFilter DA 4.0.x	Active			RHL 7.3, Red Hat ES 3.0 or 4.0
SmartFilter Control List SDK 3.x	EOL	09/2003	09/2006	Various OEM Platforms
SmartFilter Control List SDK 4.0.x	EOL	04/2004	04/2006	Various OEM Platforms
SmartFilter Control List SDK 4.1.x	EOL	05/2005	05/2007	Various OEM Platforms
SmartFilter Control List SDK 4.2.x	LOD	01/2007	01/2009	Various OEM Platforms
SmartFilter Control List SDK 4.3.x	Active			Various OEM Platforms
SmartFilter IFP SDK 2.0.x	Active			Various OEM Platforms
SmartFilter IFP SDK 3.0.x	Active			Various OEM Platforms
SmartFilter CSP SDK 4.0.x	Active			Various OEM Platforms

Internet Database of Categorized Content

Software/version	Status	LOD date	EOL date	Supported OS
	SmartFilter database			
SmartFilter 4.x XL	Active			
SmartFilter 4.x SL	Active			
SmartFilter 4.x NS	Active			
SmartFilter 3.x 3P	LOD	07/2004	12/2008	
SmartFilter 3.x 3S	LOD	07/2004	12/2008	

SmartFilter 3.x 3W	LOD	07/2004	09/2006	
SmartFilter 3.x 3M	LOD	07/2004	09/2006	
Webwasher 6.x XL	Active			
Webwasher 5.x WL	LOD	12/2006	12/2009	
Webwasher 5.x WS	Active	12/2006	12/2009	
Webwasher 5.x WD	Active	12/2006	12/2009	
		N2H2 database		
N2 2 Digest	EOL	09/2005	09/2007	
N2 Novell ICS	EOL	09/2005	09/2006	
N2 i2100 3 & 4	EOL	09/2005	09/2006	
N2 i2100 catserver	EOL	09/2005	09/2006	
N2 1 digest	EOL	09/2005	09/2006	

N2H2 Bess and Sentian Product List

Software/version	Status	LOD date	EOL date	Supported OS or application platforms
Bess i2100 Managed Service 4.0	EOL	10/2002	09/2006	Proprietary
Bess®/Sentian™ 3.5	EOL	09/2005	09/2006	WIN 2003, WIN 2000
Bess/Sentian 2.5	EOL	09/2005	09/2006	RHL 7.2 or 7.3, RHEL 2.1

ZIX Product List

See Webwasher Web Inspector above

Software/version	Status	LOD date	EOL date	Supported OS
ZIX Message Inspector	EOL	3/2005	12/2006	Windows
ZIX Web Inspector	EOL	3/2005	12/2006	Windows

Messaging Products

Hardware and Software Lifecycles

Status	HW Models	LOD date	EOL date
Active	**Generation 4** S10D, S120, E2200, E5200		
Active	**Generation 3** S10B, S25B, S50B, S100B, E2000A, E2000B, E2000C, E3000A, E3000B*, E5000A, E5000B, C10000A, C10000B	3/31/2008**	
Discontinued	**Generation 2** S10A, S25A, S50A, S100A(112)	6/30/2006	1/1/2009
Discontinued	**Generation 2** 305, 345, 345A, 345B, 345X	1/1/2005	1/1/2009
Discontinued	**Generation 1** 110,210	1/1/2004	2/19/2007

* The E3000 appliance will remain "Active" past the LOD and EOL date and will be subject to different discontinue dates.
** While supplies last.

Status	SW Version	LOD date	EOL date
Active	IronMail 6.7.x, CMC 2.7.x, Edge 2.7.x*, Encryption 6.7.x*		
Active	IronMail 6.5.x, CMC 2.5.x, Edge 2.1.x, Encryption Push/Pull	06/2008	
Maintenance	IronMail 6.1.x & 5.x, CMC 2.1.x	09/2006	07/2008
EOL	IronMail 4.1.x, CMC 1.5.x	01/2006	05/2006

* Edge 2.7.x and Encryption 6.7.x are future releases.

S10B Server Last Order Date Announcement

110/210 Server End of Life Announcement

Patches and upgrades >>

Home | Contact | Privacy Policy | Disclaimer | Sitemap

Access Control | Anti-malware | Anti-phishing | Anti-spam | Anti-spyware | Anti-virus | Application Firewall | Auditing & Reporting | Authentication | CIPA Compliance | Common Criteria | Content Filtering | Data Leakage | Email Security | Enterprise Gateway Security | Firewall | Global Intelligence | Identity Management | Internet Security | Internet Security Solutions | Intrusion Detection | Messaging Gateway Security | Messaging Security | Network Gateway Security | Network Management | Network Security | Network security software | Online Banking | Password | PCI DSS | Radius Authentication | Regulations Compliance | Remote Access | Reputation Score | Reputation System | Security Appliance | Security Audit | Security Policy | Security Software | Spam Blocker | Spam Filter | Spam Prevention | Strong Authentication | TrustedSource | Unified Threat Management | UTM Security | Virus Blocker | Virus Protection | Virus Signature | VPN | Web 2.0 Threats | Web Filtering | Web Gateway Security | Web Reputation | Web Security | Wireless Network Security

EXHIBIT 30

darkREADING
RISKY BUSINESS

Secure Computing Intros New WebWasher

Secure Computing releases next generation Web gateway security solution

SEPTEMBER 24, 2007 | SAN JOSE, Calif. – Secure Computing Corporation (Nasdaq: SCUR), a leading enterprise gateway security company, today announced the release of a new version of the company's industry-leading Webwasher® Web gateway security solution, aimed at meeting today's stringent Web security requirements. Webwasher is the only Web gateway security solution that integrates caching and security to deliver bandwidth savings and reduced latency without compromising security. Coupled with Webwasher's top-rated anti-malware engine and industry-leading TrustedSourceTM global reputation system, today's enhanced Webwasher ensures security for the Web.

"Today's bi-directional Web 2.0 environment continually introduces new and unknown threats," said IDC Research Manager, Brian Burke. "Through the use of popular Web 2.0 technologies and applications, unknown threats can enter networks through seemingly legitimate Web sites and proprietary information can exit a company with the click of a mouse. For these reasons, web gateway security should be a priority for any corporation working in a Web 2.0 environment."

The new version of Webwasher includes the following features:

- SecureCache™ integrates caching and security to deliver bandwidth savings and reduced latency without compromising security. The business requirements for caching have changed dramatically since they were first developed, and today caching introduces an array of new challenges to providing secure content. Webwasher's unique SecureCache design is the most efficient available, delivering significant improvements in caching when compared to legacy solutions.

- Anti-Malware Engine for Web threats scans traffic to analyze its intent or predicted behavior. Webwasher is able to proactively protect against spyware, day-zero blended threats and targeted attacks. Solutions that rely solely on signature updates or heuristics cannot provide this level of security. Webwasher combines this threat protection against unknown malware with the exceptional performance of a signature-based anti-virus engine for known malware threats to provide the industry's best Web gateway defense against malware as illustrated in independent studies.

- Reputation-based Filtering powered by TrustedSource, is continually enhanced and updated as the threat landscape changes. Webwasher is now able to identify and assign reputations to new domains and URLs which do not yet have content, and consequently can't be categorized. So as spammers, phishers, and others are planning their next exploit, TrustedSource proactively assigns a malicious-intent reputation score based on factors including server location, relation to other IPs and behavior of related servers. This enables customers to protect their networks by Web reputation before an exploit is launched.

- Secure Administration to meet Audit and Compliance Requirements. Webwasher appliances now ship with SafeWord® two-factor authentication tightly integrated to provide secure, proof-positive access to administration of the Web gateway. Customers can expand their deployment of SafeWord to remote users or to their entire organization with the purchase of additional SafeWord tokens.

- Webwasher SSL Scanner fills a serious security gap in the corporate IT wall of defense. Webwasher SSL Scanner denies hackers, viruses, and malicious content hidden in SSL-encrypted traffic access to the network. By scanning SSL (HTTPS) traffic and certificate updates, Webwasher enables enterprises to apply all of the advanced Webwasher protection filters, along with their existing security and Internet usage policies, to all encrypted traffic.

- Data Leakage Protection protects organizations from outbound threats such as leakage of confidential information across all key Web protocols. Webwasher provides this by performing unique outbound scanning of content to prevent intellectual property loss, comply with regulatory requirements, and provide reporting for compliance as well as forensics in the event of leakage. For advanced DLP requirements, Webwasher integrates with third-party DLP engines.

"Wide adoption of Web 2.0 applications, the increasing number of web-based attacks, and growing use of SSL have all driven the need for Web security and data leakage protection for Web traffic," said Tim Roddy, director of product marketing for Secure Computing. "What we're delivering with Webwasher is the ability for companies to operate in a Web 2.0 world while meeting these threats head on."

Secure Computing Corp. (Nasdaq: SCUR)

EXHIBIT 31

Proactive Security

Locally stored patents are here (you need the Internetiff browser plug-in to view the multipage TIFF In

Patent lists

- Computer Associates: All patents
- Computer Associates Think: All patents
- Finjan Software, Ltd.: All patents
- Trend Micro Incorporated: All patents
- Network Associates: All patents

Patents describing a proactive security system

- US Patent 5,983,348 - **"Computer network malicious code scanner", Trend Micro**
  A network scanner for security checking of application programs (e.g. Java applets or Active X c over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. S the HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-pos sequence or otherwise. The instrumented applet is then transferred to the client (web browser) to, security monitoring code. During run time at the client, the instrumented instructions are thereby security policy violations, and execution of an instruction is prevented in the event of such a viol
  1. A method of detecting and preventing execution of instructions in an application program prov computer network, comprising: providing the application program over the computer network; d whether the provided application program includes any instructions that are members of a particu instructions; *executing* the application program if it is determined that no members of the set are application program; if it is determined that an instruction is a member of the set, then altering th program, thereby allowing monitoring of execution of the instruction, wherein the altering incluc first predefined call before the instruction and a second predefined call after the instruction; and or second predefined call changes a session state of the application program.
- US Patent 6,272,641 - **"Computer network malicious code scanner method and apparatus",** (Sub-patent of 5,983,348)
  A network scanner for security checking of application programs (e.g. Java applets or Active X c over the Internet or an Intranet has both static (pre-run time) and dynamic (run time) scanning. S the HTTP proxy server identifies suspicious instructions and instruments them e.g. a pre-and-pos sequence or otherwise. The instrumented applet is then transferred to the client (web browser) to, security monitoring code. During run time at the client, the instrumented instructions are thereby security policy violations, and execution of an instruction is prevented in the event of such a viol
  1. A method of detecting and preventing execution of *problematic* instructions in an application from a computer network *to a client*, comprising: providing the application program over the cor determining, prior to downloading the application program to the client, whether the provided ap program includes any instructions that are members of a particular set of instructions; *downloadi* program without alteration and *executing* the application program if it is determined that no mem are included in the application program; if it is determined that an instruction is a member of the *downloading* the application program to the client along with a *security monitoring package*, the monitoring of execution of the instruction at the client.

- US Patent 6,154,844 - **"System and method for attaching a downloadable security profile to downloadable", Finjan**
  A system comprises an inspector and a protection engine. The inspector includes a content inspe

Plaintiff's Trial Exhibit
PTX-38
Case No. 06-369 GMS

EXHIBIT
38
GERMANY
PENGAD 800-631-6989

uses a set of rules to generate a Downloadable security profile corresponding to a Downloadable,
applets, ActiveX.TM. controls, JavaScript.TM. scripts, or Visual Basic scripts. The content inspe
links the Downloadable security profile to the Downloadable. The set of rules may include a list
operations, or a list of suspicious code patterns. The first content inspection engine may link to tl
a certificate that identifies the content inspection engine which created the Downloadable securit
Additional content inspection engines may generate and link additional Downloadable security p
Downloadable. Each additional Downloadable security profile may also include a certificate that
creating content inspection engine. Each content inspection engine preferably creates a Downloa
identifies the Downloadable to which the Downloadable security profile corresponds. The protec
Downloadable interceptor for receiving a Downloadable, a file reader coupled to the interceptor
whether the Downloadable includes a Downloadable security profile, an engine coupled to the fi
determining whether to trust the Downloadable security profile, and a security policy analysis en
the verification engine for comparing the Downloadable security profile against a security policy
determines that the Downloadable security profile is trustworthy. A Downloadable ID verificatio
retrieves the Downloadable ID that identifies the Downloadable to which the Downloadable secu
corresponds, generates the Downloadable ID for the Downloadable and compares the generated I
the linked Downloadable. The protection engine further includes a certificate authenticator for au
certificate that identifies a content inspection engine which created the Downloadable security pr
trusted source. The certificate authenticator can also authenticate a certificate that identifies a de
created the Downloadable.
1. A method comprising: receiving by an inspector a Downloadable; generating by the inspector
Downloadable security profile that identifies suspicious code in the received Downloadable; and
inspector the first Downloadable security profile to the Downloadable before a web server make
Downloadable available to web clients.

- US Patent 6,092,194 - **"System And Method For Protecting a Computer and a Network Fro
  Downloadables", Finjan** (SurfinGate behavior-inspection of code at the gateway)
  A system protects a computer from suspicious Downloadables. The system comprises a security
  interface for receiving a Downloadable, and a comparator, coupled to the interface, for applying
  policy to the Downloadable to determine if the security policy has been violated. The Download
  a Java.TM. applet, an ActiveX.TM. control, a JavaScript.TM. script, or a Visual Basic script. Th
  may include a default security policy to be applied regardless of the client to whom the Downloa
  addressed, or a specific security policy to be applied based on the client or the group to which th
  The system uses an ID generator to compute a Downloadable ID identifying the Downloadable,
  fetching all components of the Downloadable and performing a hashing function on the Downlo
  the fetched components. Further, the security policy may indicate several tests to perform, includ
  comparison with known hostile and non-hostile Downloadables; (2) a comparison with Downloa
  blocked or allowed per administrative override; (3) a comparison of the Downloadable security p
  against access control lists; (4) a comparison of a certificate embodied in the Downloadable agai
  certificates; and (5) a comparison of the URL from which the Downloadable originated against t
  untrusted URLs. Based on these tests, a logical engine can determine whether to allow or block t
  Downloadable.
  1. A computer-based method, comprising the steps of: receiving an incoming Downloadable add
  by a server that serves as a gateway to the client; comparing, by the server, Downloadable securi
  pertaining to the Downloadable, the Downloadable security profile data includes a list a suspicio
  operations that may be attempted by the Downloadable, against a security policy to determine if
  policy has been violated; and preventing execution of the Downloadable by the client if the secu
  been violated.
- US Patent **6,167,520 - "System And Method For Protecting a Client From Hostile Downloa**
  (SurfinShield desktop Sandboxing technology)

A system and method examine execution or interpretation of a Downloadable for operations deei hostile, and respond accordingly. The system includes security rules defining suspicious actions : policies defining the appropriate responsive actions to rule violations. The system includes an int receiving incoming Downloadable and requests made by the Downloadable. The system still furt comparator coupled to the interface for examining the Downloadable, requests made by the Dow runtime events to determine whether a security policy has been violated, and a response engine c comparator for performing a violation-based responsive action.
1. A computer-based method, comprising: monitoring the operating system during runtime for ar from a request made by a Downloadable; interrupting processing of the request; comparing infor to the Downloadable against a predetermined security policy; and performing a predetermined re based on the comparison, the predetermined responsive action including storing results of the coi event log.

- US Patent 6,480,962 - **"System and method for protecting a client during runtime from host downloadables", Finjan** (SurfinShield desktop Sandboxing technology, same as 6,167,520 but subsystems of the operating system)
A system protects a client from hostile Downloadables. The system includes security rules defini actions and security policies defining the appropriate responsive actions to rule violations. The sy interface for receiving incoming Downloadable and requests made by the Downloadable. The sy includes a comparator coupled to the interface for examining the Downloadable, requests made t Downloadable and runtime events to determine whether a security policy has been violated, and coupled to the comparator for performing a violation-based responsive action.
1. A computer-based method, comprising: monitoring substantially in parallel a plurality of subs operating system during runtime for an event caused from a request made by a Downloadable; in processing of the request; comparing information pertaining to the Downloadable against a prede policy; and performing a predetermined responsive action based on the comparison.

Patents describing an algorithm to detect hostile executables

- US Patent 6,449,723 **"Method and system for preventing the downloading and execution of objects", Computer Associates Think** (Scanning the header of downloads if they will utilize fo resources)
A method for selectively preventing the downloading and execution of undesired Executable Ob computer includes analyzing a header of a an Executable Object which is detected at a gateway, resources of a computer that the Executable Object needs to utilize and comparing the resources that the Executable Object needs to utilize with a user's Security Policy representing the resource combination of resources, that the user allows or does not allow an executable object to utilize w The Executable Object is allowed to pass through the gateway and to reach the computer which l downloading, if the resources of the computer that the Executable Object needs to utilize are incl the resources allowed for use by the Security Policy. The Executable Object is prevented from pa gateway, thereby preventing it from reaching the computer which has initiated its downloading, i the computer that the Executable Object needs to utilize are included in the list of the resources p by the Security Policy.
- US Patent 6,336,140 - **"Method and system for the identification and the suppression of exec Computer Associates Think** (Rarranges the requested objects of a Web page in a sequential ord by 6,449,723)
A method for processing Executable Objects, comprising: (a) providing analysis means capable c analysis of data packets transmitted on a communication line between a browser and an HTTP se said communication line being established through a gateway; (b) analyzing the handshake betw and said server, to detect a "GET_" command sent by the user and an HTTP code sent in respons

(c) when such an HTTP code is detected, analyzing the data packets transmitted by said server tc by: (c.1) providing ordering means to order data packets received in non-sequential order, and to sequential order to header checking means; (c.2) checking the data packets so as to analyze the c header of the Executable Object, and to identify the resources of the system that it needs to empl transmitting to said gateway data representing the resources of the system that the Executable Ot utilize; (c.4) providing data packet suppressing means coupled to said gateway, such that if the re system that the Executable Object needs to utilize are not permitted according to the security pol administrator, at least one data packet belonging to the Executable Object is suppressed, altered to prevent the execution thereof by the browser.

Other

- US Patent **5,623,600** - **"Virus detection and removal apparatus for computer networks", Tr** (Scanning of viruses on the gateway for FTP and SMTP) {RCy: This is a strong patent cited by r patents}
  A system for detecting and eliminating viruses on a computer network includes a File Transfer P proxy server, for controlling the transfer of files and a Simple Mail Transfer Protocol (SMTP) pr controlling the transfer of mail messages through the system. The FTP proxy server and SMTP p concurrently with the normal operation of the system and operate in a manner such that viruses tr from the network in files and messages are detected before transfer into or from the system. The and SMTP proxy server scan all incoming and outgoing files and messages, respectively before t viruses and then transfer the files and messages, only if they do not contain any viruses. A methc a file before transmission into or from the network includes the steps of: receiving the data transf file name; transferring the file to a system node; performing virus detection on the file; determini file contains any viruses; transferring the file from the system to a recipient node if the file does r virus; and deleting the file if the file contains a virus.
- US Patent **6,701,440** - **"Method and system for protecting a computer using a remote e-mail device", Network Associates**
  (Virus scanner at the gateway for emails) {RCy: patent is from March 2004, overlaps with **5,623**
  A system and method for a remote or network-based application service offering virus scanning, detecting of e-mail viruses prior to the e-mail messages arriving at the destination system or serv The method protects a computer system that is configured to receive an e-mail message addresse e-mail address from viruses in an incoming e-mail message. The method generally includes recei incoming e-mail message at a remote e-mail receiving server, scanning the e-mail message for vi the e-mail message if it is clean to a remote e-mail sending server, attempting to clean the e-mail infected to generate a cleaned e-mail message, forwarding the cleaned e-mail message, if any, to sending server, and forwarding the clean or cleaned e-mail message, if any, to the destination e-n the remote e-mail sending server. The system generally includes a remote e-mail receiving server incoming e-mail message, a virus-detection program for scanning the e-mail message for virus, a virus processing server for attempting to clean the infected e-mail message, and a remote e-mail forwarding the clean or cleaned e-mail message, if any, to the destination e-mail address.

- US Patent **6,553,498** - **"Method and system for enforcing a communication security policy", Associates Think** (Assures that downloadable is only delivered from a gateway to a client if the security agent installed)

- US Patent **6,611,925** - **"Single point of entry/origination item scanning within an enterprise Network Associates** (ID attached to scanned objects to avoid rescan, overlaps with Finjan **6,154**
  A method and system for on-access virus scanning within an enterprise or in a workgroup, where

authenticated against a trusted certificate authority. The first time an item, such as an executable is accessed, it is scanned for viruses, worms, trojan horses, or other malicious code, and, after the determined to be free from threats or is corrected, a certificate noting this information is generate time a Globally Unique Identifier ("GUID") is generated and appended to the item. The certificat various information, including the identity of the scanner that performed the virus check, as well determining if the original item has been altered since it was scanned, and is stored in a certificat GUID is used as a pointer for locating the certificate. A subsequent user who accesses the item w GUID and can use the GUID to locate the certificate for the item. If the certificate can be located tampered with and the item has not been changed since it was scanned, the subsequent user can a without re-scanning it.

- US Patent 6,338,141 - **"Method and apparatus for computer virus detection, analysis, and r time", CyberSoft, Inc.**
  A method and apparatus for detecting computer viruses comprising the use of a collection of rela detect computer viruses in computer files. The collection of relational data comprises various rel: objects created from viruses. Computer files, as they are checked for viruses, are run through a p: those relational signature objects. Those objects created from the file are then checked against th relational data. Depending on the results, the file may be infected and prohibited from running or method may be performed on a single, stand-alone computer system in real time, as well as a net

- US Patent 6,721,424 **"Hostage system and method for intercepting encryted hostile data", C**
  (Allows to inspect encrypted content by a key storage) {RCy: This is another SSL-Scanner Meth A method for intercepting data transmissions in a system which is comprised of an external netw computers within a protected local network. A proxy server located in the communication path, t external network and the computers, is equipped with virus detection capability and includes, als means and a hostage storage facility. If the proxy server determines that an incoming transmissic external network contains hostile data, a key is obtained from the key storage means so as to dec: transmission. If no such key is available, the proxy server prevents the data transmission from en protected network and stores the data transmission as "hostage data" within the hostage storage f intended user provides the proxy server with a key capable of decrypting the hostage data transm

- **US Patent 6,577,920 - "Computer virus screening", Data Fellows Oyj**
  A method of screening a software file for viral infection comprising defining a first database of k virus signatures, a second database of known and certified commercial macro signatures, and a tl known and certified local macro signatures. The file is scanned to determine whether or not the f macro. If the file contains a macro, a signature for the macro is determined and screened against contained in said databases. A user is alerted in the event that the macro has a signature correspo signature contained in said first database and/or in the event that the macro has a signature which correspond to a signature contained in either of the second and third databases.

Ideas

	Webwasher	**Trend Micro**	**Finjan**
Static scanning	gateway or client	gateway (or client)	gateway
block if unassigned or untrusted certificates		Java	Java
block if authenticode signature is not in MS Internet Explorer or set as untrustful in		ActiveX	ActiveX

IE (according to IE on client????)			
block if viruses (signatures)		?	optional McAf
block if hash code blacklisted by administrator	Java, ActiveX (Webwasher 5.0)	Java	{yes}
block if hash code blacklisted by system (violated a policy on the client in the past) (automatically added to blacklist from admin)		Java (default setting is 'turned off')	?
block if hash code blacklisted by vendor (automated updates)		Java, ActiveX	none
block if downloadable requested from blacklisted URL (list maintained by admin)	Java, ActiveX, Javascript, VBscript, ... (Webwasher 5.0)	Java, Javascript	{yes}
completely block the following file types	Java, ActiveX, Javascript, VBScript, ... (Webwasher 5.0)	Java, Javascript, ActiveX, VBScript	{yes}, filetype only, no magic archives
isolate suspicious commands and pass to client (watcher code injected in downloadable)		Java	no
run time monitoring		client	client
requires installation on client	no	no	yes, exchanges libraries (requi individual pacl each browser t version)
executes downloadable incl. watcher code		Java	no
terminate downloadable if instruction violates policy		Java	Java
policy: a security weight of a session is exceeded (the overall activity of the downloadable seems to be too dangerous)		Java	no
policy: file operations (e.g. READ, WRITE, DELETE, RENAME)		Java (access hard drive, CPU, Windows, network resources, ...)	
policy: network operations (LISTEN on socket, CONNECT to a asocket, SEND data, RECEIVE data, VIEW INTRANET)		Java	
policy: registry operations (READ, WRITE)		Java	
policy: operating system operations (EXIT WINDOWS, EXIT BROWSER, START or KILL or CHANGE		Java	

PROCESS/THREAD, PRIORITY, DYNAMICALLY LOAD A CLASS)			
policy: resource usage thresholds (memory, CPU, graphics)		Java	
send notification to administrator (email)		Java	
automatically add signature of hostile downloads to blacklist		Java (MD5 digest valuesignature)	yes (cannot be
automatically send signature of hostile downloads to vendor for inspection		Java	Java
check invoked downloadables already on client		no	no
block applications on client		no	yes
Security Policy	dynamically retrieved, flexible	injected in downloadable, fixed	
multiple policies		user, groups	user, groups
authentication			NTLM/Active Support
Reporting			
logfiles		yes	yes
reports		yes	yes
administration		browser-based, Windows based	Windows-base
single point of management for multiple distributed servers			yes
Other			
protocols		HTTP 1.0	independent oı
performance		max. 500 concurrent users	max. 5000 use reuests/sec)
high availibility		if server fails, then clients are no longer protected	If server fails t are still protec locally stored : policy.
secures downloadable with own signature		Java (simplifies roll-out. Only one signature needs to be trusted on client)	Java
compatibility problems		no HTTP 1.1	
Platforms			
OS server		Windows, Solaris	Windows 200(
OS database server		none	Windows 200(
OS client		none	Windows

Integration		Check Point Firewall-I (OPSEC)	Check Point's ! Microsoft's IS, firewall/Web c server, MS Prc Cisco's PIX Fi

Literature

- Poison Java, Eva Chen, CTO Trend Micro, 1999
- It's Time to Rethink your Corporate Malware Strategy
- Microsoft ActiveX {RCy: poor}

Securing ActiveX

- Exploder FAQ: An ActiveX control is essentially a Windows program that can be distributed fro {RCy: Nice. Discusses dangers, authenticode etc.}
- Security Tradeoffs: Java vs. ActiveX
- ActiveX Security: Exploring and Exploiting Code Download [local]

Products

- **Trend Micro AppletTrap**
- **SurfinShield Corporate 5.7 from Finjan Software** Until recently, Finjan has offered only an Ir product and a desktop version designed for home use. The Corporate Edition (which is new) is d business environments, and includes a central database control unit, and client modules. The cen corporate, group-level, and local security policies, and incorporates extensive logging and centra capabilities. The software can accommodate different profiles, so administrators can allow variou non-malicious ActiveX content to flow to the end user. This is called "white listing". A sandbox by Finjan to control access to the file system and registry. Signature scanning is provided througl with F-Secure. Malicious macros are not addressed.
- **eSafe Enterprise by Aladdin Knowledge Systems, Inc.** This product incorporates its own signa antivirus scanner as well as application-specific and general purpose sandboxing. It also offers a and built-in file integrity checker. Heuristic scanning identifies new malicious macros as they are When installed on a server, consolebased deployment is supported, and security configurations c by individual users and groups. Centralized reporting and alerting is included as well. This is a v comprehensive product with a wide variety of features.
- **Pelican SafeTNet 2.0 from Pelican Security, Inc.** Like other products, this one detects and isol malicious active content. But unlike Finjan, the product lets users secure applications and system who has access to make changes. It blocks content by determining what can be changed, as oppo be let through. Like other behavior-blocking tools, the SafeTnet software builds a sandbox aroun other code that is downloaded. Unlike Aladdin's sandbox technology, the company claims that it: dynamic approach in that the sandbox is only run when active content is downloaded, thus savin; The product uses SNMP traps to allow integration with enterprise management frameworks such OpenView.
- **Secure4U by Sandbox Security** This is another product incorporating sandboxing. Its policy-ba are similar to those of Windows NT security access control lists, allowing system administrators

consistent network-wide access policy. An interface is provided to allow conventional signature with a third-party product. A personal firewall is included. Malicious macros are not addressed.

- **Achilles' Shield by InDefense, Inc.** This product is similar to SafeTnet, although it incorporates protection for system sectors, a module for scanning known viruses, and a function for detecting conventional memory. The product includes a built-in file integrity checker which can detect una modifications. Any macros present are checked against the policy database and are locked out ur certified.
- **Stormwatch by Okena Stormwatch** doesn't look at specific threats, or specific code, but at ove performance. It checks every command, network, or system registry operation for any deviance f system behavior. Stormwatch combines behavior analysis with static and dynamic heuristics.

Risks:

- Microsoft Longhorn employs sandbox: SEE (Secure Execution Environment). The TrustManage component, evaluates the requested permissions for potential risk (for example, IsolatedStorage j risky than general FileIO permission), and then the available evidence (Authenticode signature, z etc.) to arrive at a trust decision.

Controls built with .NET run within a secure client-side sandbox -- so that they can be prevented from : attacking a users client system (so that it has none of the security concerns that activex controls have to downloaded they are also cached on the client machine -- enabling you to have to re-download them ag to the page. The client-side technology to easily create these types of client controls in .NET is called " lives within the System.WinForms code namespace. It has built-in designer support within Visual Stud details on how to use .NET Client Controls within a browser can be found in this article: http://www.gotdotnet.com/team/windowsforms/iesourcing.aspx

Last Update: 29-Jun-2004 roland.cuny@webwasher.com
©2000-2003 Roland Cuny

EXHIBIT 32

Print This Article

<< Return to Secure Computing Webwasher 6.0

Secure Computing Webwasher 6.0

Peter Stephenson
2/1/2007

Adjust Font Size: A | A | A

Product Information

Vendor:Secure Computing
Product:Webwasher 6.0
Website:www.securecomputing.com
Price:$8,613 for 250 users

Product Rating

Features	★★★★★
Ease of Use	★★★★★
Performance	★★★★★
Documentation	★★★★☆
Support	★★★★★
Value for Money	★★★☆☆
Overall Rating	★★★★★

For:

Highly customizable and very flexible as well as feature rich.

Against:

Requires proxy connections that could impact performance and large environments; can become pricey.

Verdict:

Strong product for larger organisations, very flexible

Related Group Test

Web content filtering 2007

Reviews For This Vendor

Secure Computing Webwasher 6.0 is a strong product in almost every regard. We especially liked its ability to perform individual analysis on words, phrases and scanned images. This goes well beyond typical blacklists for URL blocking and keyword lists for filtering. We found ease-of-use excellent and the product contains features, some of which are not usually found in this type application. Webwasher is delivered as an appliance.

Set-up and initial configuration are made easy by Secure Computing's "set-up assistant." This creates a configuration file that you load into the device. The user interface uses tab style menus that make for easy navigation and intuitive use. While the policy engine has predefined policies, the administrator can easily customize or create new policies using drop-down menus.

Webwasher goes well beyond usual URL blocking and keyword filtering by using pattern matching to adapt filters and to perform analysis on words and phrases. The appliance sits at the network gateway and monitors all inbound and outbound connections. In addition to the URL filter and word analysis filters, the appliance contains anti-malware, anti-virus, anti-spam, content protection, SSL scanning and IM filtering.

Documentation is above average and is provided as several PDF documents. These documents are separated into separate files for the configuration of different components, such as the installation of the appliance, installation of content reporter and system configuration. There also are several user guides which detail the use and the functions of system components.

Support for Webwasher is first rate. The support area of the website includes product activation, patches, upgrades and product documentation. Online support for technical issues, a knowledge base and 24/7 telephone email support also are available.

Pricing for Webwasher is a bit complex and can be somewhat expensive for larger organizations. The appliance has a base price and, in addition, each module is priced as a subscription. Intended for larger organizations, the product comes in three platforms. The smallest platform supports up to 4,000 users while the largest supports up to 16,000. Pricing increases with the size of the platform. Volume discounts provide some pricing improvement for larger organizations.